



Dhīmahī Technolabs

Cybersecurity Essentials Checklist

 www.dhimahitechnolabs.com

 hello@dhimahitechnolabs.com

Cybersecurity Essentials Checklist

Description: Essential cybersecurity measures every small business should implement. Includes free tools recommendations and security audit template.

Context: India (SMEs in Gujarat, Maharashtra, Delhi-NCR, Bengaluru, etc.).

Table of Contents

Part I — Foundations

1. Introduction
2. Why Cybersecurity Matters for Indian SMEs
3. Common Cyber Threats in India

Part II — Core Essentials

4. Passwords & Authentication
5. Device & Network Security
6. Data Backup & Recovery
7. Email & Phishing Protection
8. Software & Patch Management
9. Cloud & SaaS Security
10. Mobile & Remote Work Security

Part III — Governance & Training

11. Employee Awareness & Training
12. Legal & Regulatory Compliance (India Context)
13. Incident Response Planning

Part IV — Practical Tools & Templates

14. Free Tools & Indian Alternatives
15. Cybersecurity Audit Template
16. Implementation Roadmap for SMEs

Appendices

- Glossary
- Vendor Directory (India-Focused)
- About Dhīmahī Technolabs

Part I — Foundations

1. Introduction

Cybersecurity is no longer optional. For **small businesses in India**, threats like phishing, ransomware, and data breaches are increasing. SMEs in Gujarat, Delhi, or Bengaluru may think hackers target only large companies, but in fact **SMEs are easier targets** due to weaker defenses.

This checklist provides:

- **Essential practices** every small business should adopt.
- **Free and affordable tools** in the Indian context.
- **Audit templates** to check your organization's readiness.

2. Why Cybersecurity Matters for Indian SMEs

- **Financial Losses:** Ransomware demands can range from ₹50,000 to several lakhs.
- **Reputation Damage:** Loss of customer trust.
- **Compliance Risks:** Under India's **DPDP Act 2023**, mishandling customer data can lead to penalties.
- **Business Continuity:** A data breach can halt operations for days.

3. Common Cyber Threats in India

- **Phishing Emails** (fake GST/UPI notices).
- **Ransomware Attacks** on healthcare, finance, and manufacturing SMEs.
- **WhatsApp Scams** targeting customer service channels.
- **Data Leaks** from unsecured cloud accounts.
- **Insider Threats**: Employees misusing or leaking data.

Part II — Core Essentials

4. Passwords & Authentication

- Enforce **strong passwords** (min 12 characters, mix of symbols).
- Use **Multi-Factor Authentication (MFA)**, especially for email, banking, CRM.
- Deploy **password managers** (e.g., Bitwarden free, KeePass).

✅ *Tip: Encourage staff to use Hindi/Gujarati words + symbols for memorable strong passwords.*

5. Device & Network Security

- Install **antivirus** (Quick Heal, K7 Security, or free Microsoft Defender).
- Use **firewalls**: Router + software firewall.
- Secure Wi-Fi with WPA3, not default passwords.
- Isolate guest Wi-Fi from company network.

6. Data Backup & Recovery

- Follow **3-2-1 rule**: 3 copies, 2 media, 1 offsite.
- Use **cloud backups** (Google Drive, OneDrive, Zoho WorkDrive).
- Test restores quarterly.

7. Email & Phishing Protection

- Use **SPAM filters** (Zoho Mail, ProtonMail, Outlook).
- Train staff: Verify GST/UPI messages before clicking.
- Enable **DKIM, SPF, DMARC** for your business domain.

8. Software & Patch Management

- Enable **automatic updates** for Windows, Linux, macOS.
- Maintain an **inventory of all software**.
- Remove unused apps/plugins (especially WordPress SMEs).

9. Cloud & SaaS Security

- Restrict access: **role-based permissions**.
- Use **SaaS with Indian servers** if handling personal data.
- Monitor file sharing on Google Drive/Zoho.

10. Mobile & Remote Work Security

- Enable **screen locks & encryption**.
- Install **mobile antivirus** (free Avast/Kaspersky).
- Avoid public Wi-Fi for UPI/banking transactions.
- Use **VPN** (ProtonVPN free, or Indian VPN vendors).

Part III — Governance & Training

11. Employee Awareness & Training

- Monthly 30-min sessions on phishing, WhatsApp scams.
- Posters in Gujarati/Hindi: “Don’t click unknown links.”
- Conduct **phishing simulations**.

12. Legal & Regulatory Compliance (India)

- **DPDP Act 2023**: Consent required for personal data.
- **IT Act 2000**: Governs electronic records.
- **SEBI/IRDAI Guidelines** for financial SMEs.
- Maintain **audit logs** for 2–3 years.

13. Incident Response Planning

- Define roles: Who contacts CERT-In, who talks to customers?
- Keep **24/7 emergency contacts**.
- Steps: Detect → Contain → Eradicate → Recover → Review.

- Test incident drills yearly.

Part IV — Practical Tools & Templates

14. Free Tools & Indian Alternatives

- **Antivirus:** Quick Heal (paid, India), Microsoft Defender (free).
- **Firewall:** pfSense (open-source).
- **Backup:** Zoho WorkDrive (Indian SaaS), Google Drive free.
- **Password Management:** Bitwarden free, KeePass.
- **Phishing Simulation:** Gophish (open-source).
- **VPN:** ProtonVPN free, IndianVPN.

15. Cybersecurity Audit Template

Cybersecurity Audit Checklist (Sample)

Category	Yes/No	Notes
Strong passwords enforced		
Multi-Factor Authentication enabled		
Antivirus installed & updated		
Firewall active		
Regular backups tested		
Staff trained on phishing		
Domain has SPF/DKIM/DMARC		

SaaS access is role-based

Incident Response Plan tested

16. Implementation Roadmap for SMEs

Phase 1 (Month 1–2):

- Set up antivirus, firewalls, backups.
- Train staff on phishing.

Phase 2 (Month 3–4):

- Enable MFA across systems.
- Implement password manager.
- Draft Incident Response Plan.

Phase 3 (Month 5–6):

- Conduct mock phishing drill.
- Run security audit using template.
- Budget ₹50,000–₹1,50,000 annually for security upkeep.

Appendices

Glossary

- **Phishing:** Fraudulent email asking for info.
- **Ransomware:** Malware encrypting data until ransom is paid.
- **MFA:** Multi-Factor Authentication.
- **CERT-In:** Indian Computer Emergency Response Team.

Vendor Directory (India)

- Quick Heal (Pune)
- K7 Security (Chennai)
- Seqrite (enterprise arm of Quick Heal)
- Zoho WorkDrive (Chennai)
- Indian VPN providers

About Dhīmahī Technolabs

We help SMEs in Gujarat secure IT systems with affordable, practical cybersecurity setups: antivirus, cloud backup, phishing training, and compliance support.