CORPORATE TECHNOLOGIES LLC
gocorptech.com

CYBERSECURITY POLICIES FOR SMALL BUSINESS CHECKLIST

Executive Tool for Core Security Controls

Built for small business leaders and operations managers. Use this checklist to assess foundational cybersecurity policies.

How to Use

1. Takes 20–30 minutes
2. Check each box that applies
3. Count the total number of checked items
4. Identify policy and security exposure

1

Access Control Policies

- ☐ Enforce least-privilege access rules
- ☐ Limit access to sensitive data
- ☐ Approve access requests through managers
- ☐ Use role-based user groups
- ☐ Review user permissions regularly
- ☐ Audit privileged account activity

2

Employee Account Management

- ☐ Document employee onboarding process
- ☐ Disable accounts after employee departure
- ☐ Coordinate account closures with HR
- ☐ Forward email after account closure
- ☐ Transfer ownership of work data
- ☐ Audit inactive user accounts

3

Device Security Policies

- ☐ Require antivirus on all devices
- ☐ Enforce security updates on endpoints
- ☐ Apply security patches automatically
- ☐ Audit personal devices on Wi-Fi
- ☐ Restrict unmanaged device access
- ☐ Review endpoint protection status

4

Data Backup Policies

- ☐ Back up critical data daily
- ☐ Maintain three backup copies
- ☐ Use two different storage types
- ☐ Store one backup off-site
- ☐ Monitor backup job success
- ☐ Test data restoration regularly

5

Email Security Policies

- ☐ Enable advanced email filtering
- ☐ Block malicious attachments automatically
- ☐ Scan links for phishing threats
- ☐ Flag external senders clearly
- ☐ Train staff on phishing risks
- ☐ Review suspicious email reports

6

Security Policy Governance

- ☐ Document cybersecurity policies formally
- ☐ Assign policy ownership internally
- ☐ Review policies annually
- ☐ Train employees on policy rules
- ☐ Record policy acknowledgments
- ☐ Update policies after incidents

Scoring Model

- Count the total number of checked items
- Total Possible Score: 36
- 0–12 → High Risk
- 13–29 → Moderate Risk
- 30–36 → Controlled / Policy-Ready

Immediate Red Flags

- No access control policies
- Accounts active after employee departure
- Devices without antivirus protection
- No daily data backups
- No email phishing protection
- No written security policies

Next Step

If your score indicates exposure, schedule a Cybersecurity Policy Review.

Cybersecurity Policy Review