CORPORATE TECHNOLOGIES LLC
gocorptech.com

SMALL BUSINESS CYBERSECURITY CHECKLIST

Executive Tool for Essential Security Controls

Built for business owners and operations leaders. Use this checklist to assess core cybersecurity protections.

How to Use

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

1 Security Foundations

- ☐ Document cybersecurity policies
- ☐ Assign internal security ownership
- ☐ Review cybersecurity risks annually
- ☐ Define incident response procedures
- ☐ Record security audit findings
- ☐ Update policies after incidents

2 Identity & Access Security

- ☐ Require multi-factor authentication
- ☐ Use role-based access permissions
- ☐ Review user access quarterly
- ☐ Disable inactive user accounts
- ☐ Restrict admin privileges carefully
- ☐ Audit privileged account activity

3 Endpoint & Device Protection

- ☐ Install antivirus on all endpoints
- ☐ Enable automatic system updates
- ☐ Encrypt laptops and mobile devices
- ☐ Monitor endpoint security status
- ☐ Restrict unauthorized software installs
- ☐ Audit unmanaged devices regularly

4 Network Security Controls

- ☐ Configure firewall protection rules
- ☐ Segment sensitive network systems
- ☐ Monitor network traffic anomalies
- ☐ Disable unused ports and services
- ☐ Secure Wi-Fi access controls
- ☐ Audit router and firewall settings

5

Threat Monitoring & Detection

- ☐ Enable real-time threat monitoring
- ☐ Configure alerts for suspicious activity
- ☐ Log system security events
- ☐ Review intrusion alerts regularly
- ☐ Track unusual login patterns
- ☐ Investigate abnormal system behavior

6

Backup & Recovery Protection

- ☐ Back up critical data daily
- ☐ Store backups offsite or cloud
- ☐ Monitor backup job success
- ☐ Test restoration procedures regularly
- ☐ Document disaster recovery plan
- ☐ Assign recovery process ownership

Scoring Model

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

Immediate Red Flags

- No multi-factor authentication
- No endpoint protection installed
- No firewall security rules
- No threat monitoring alerts
- No tested data backups
- No incident response plan

Next Step

If your score indicates exposure, schedule a Cybersecurity Risk Assessment.

Cybersecurity Risk Assessment