

# IT Essentials Checklist for Small Businesses

### Instructions:

Use this checklist to assess your small business's IT infrastructure. Mark each item as **Complete**, **Needs Improvement**, or **Missing** to identify areas that require attention.

---

## 1. Hardware Inventory

- ☐ Computers, laptops, and mobile devices are up-to-date and functional.
- ☐ Networking equipment (routers, switches, modems) is secure and operational.
- ☐ Firewalls and security appliances are in place and configured properly.
- ☐ Backup devices (external hard drives, NAS, cloud-based solutions) are regularly used.
- ☐ Business-grade printers and peripherals are in good working condition.

### Notes:

---

---

---

---

## 2. Software & Licensing

[ ] All operating systems are updated and supported.

[ ] Business applications (email, productivity, accounting) are properly licensed.

[ ] Software updates and security patches are applied regularly.

[ ] Cloud-based applications (Microsoft 365, Google Workspace, CRM) are utilized effectively.

[ ] Antivirus and endpoint protection software is installed and active.

### Notes:

---

---

---

---

### 3. Cybersecurity Measures

- ☐ A firewall is installed and configured to block unauthorized access.
- ☐ Multi-Factor Authentication (MFA) is enabled for all critical accounts.
- ☐ Employees use strong, unique passwords and a password manager.
- ☐ Regular cybersecurity training is provided to employees.
- ☐ Anti-malware and phishing protection tools are in place.
- ☐ Secure Wi-Fi networks with strong encryption are used.

**Notes:**

---

---

---

---

### 4. Cloud & Backup Solutions

- ☐ All critical business data is backed up regularly.
- ☐ Backups are stored both onsite and in a secure cloud service.
- ☐ A disaster recovery plan is documented and tested.
- ☐ Cloud storage solutions are used for secure file sharing.
- ☐ Data access permissions are managed to limit exposure.

**Notes:**

---

---

---

---

## 5. IT Support & Maintenance

[ ] A designated IT support provider or in-house IT team is available.

[ ] IT policies and procedures are documented and accessible.

[ ] Proactive IT monitoring and maintenance are in place.

[ ] Cybersecurity incident response plan is established.

[ ] Regular IT reviews and audits are conducted to ensure best practices.

### Notes:

---

---

---

---

### Next Steps:

- Review the checklist and prioritize areas marked as **Needs Improvement** or **Missing**.
- Take corrective actions to strengthen your IT infrastructure.
- **Schedule a free consultation with Hotline Helpdesk** for expert recommendations and support. [brandon@hotlinehelpdesk.com](mailto:brandon@hotlinehelpdesk.com)