

**SMALL BUSINESS IT GUIDE**

# The Small Business IT Starter Kit

What a business under 50 people genuinely needs in place - and what vendors will try to sell you that you do not.

|           |                                                         |
|-----------|---------------------------------------------------------|
| <b>01</b> | <b>The security baseline every small business needs</b> |
| <b>02</b> | <b>Backup and recovery sized for a small team</b>       |
| <b>03</b> | <b>How to tell useful IT spend from padding</b>         |

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

**Prepared by Brotherly Technology**

Owner-led IT, security, and compliance support.

## 15-MINUTE ASSESSMENT

# Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

|                                                                                                                            |                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Every user has a unique account, MFA, approved password management, and no routine admin rights.  | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> New-hire, role-change, and departure checklists have named approvers and timing.                  | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Business devices use supported software, encryption, managed protection, auto-lock, and patching. | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Email has phishing protection, domain authentication, and a simple report button or process.      | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Firewall, Wi-Fi, guest access, remote access, and network equipment are documented and supported. | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Files live in approved business storage with role-based access and controlled sharing.            | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Critical cloud and onsite data is backed up separately from ordinary sync and retention.          | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> A restore test proves the team can resume within agreed RTO and RPO targets.                      | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Users know one support path and urgent issues have a human escalation route.                      | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Inventory, vendors, licenses, warranties, renewals, and administrator credentials are owned.      | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Payment changes and sensitive requests require verification through a known separate channel.     | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |
| <input type="checkbox"/> Incident, outage, and departure procedures are short, current, and accessible offline.            | <input type="checkbox"/> Yes<br><input type="checkbox"/> Partial<br><input type="checkbox"/> No |

**Quick score:** Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

## RIGHT-SIZED BASELINE

# Cover the essentials before buying another dashboard

A small team needs clear ownership and broad controls more than an oversized tool stack.

| Priority        | Minimum capability                                                   | Proof                                 |
|-----------------|----------------------------------------------------------------------|---------------------------------------|
| <b>Identity</b> | Unique accounts, MFA, password manager, least privilege, offboarding | Coverage and access review            |
| <b>Devices</b>  | Supported, encrypted, patched, protected, inventoried                | Health and patch report               |
| <b>Email</b>    | Filtering, authentication, reporting, payment verification           | Domain checks and test report         |
| <b>Network</b>  | Supported firewall/Wi-Fi, guest separation, secure remote access     | Diagram, configuration backup, review |
| <b>Data</b>     | Approved storage, controlled sharing, retention decision             | Permission and sharing report         |
| <b>Recovery</b> | Independent backup, isolated copy, tested RTO/RPO                    | Restore exercise results              |
| <b>Response</b> | Human escalation, incident contacts, alternate communication         | Runbook and tabletop record           |

Start with controls that reduce several risks at once. MFA, offboarding, managed devices, payment verification, and tested recovery are high-leverage choices.

**BUDGET DISCIPLINE**

# Separate useful IT spend from padding

Pay for a measurable capability, accountable owner, coverage evidence, and operating process - not a product name alone.

|   |                                                                                                                                      |
|---|--------------------------------------------------------------------------------------------------------------------------------------|
| 1 | List the business outcome for each tool or service: uptime, protection, recovery, support, compliance, collaboration, or efficiency. |
| 2 | Record who owns it, which users/devices/systems it covers, what report proves operation, and what happens when it fails.             |
| 3 | Find overlap in endpoint, email, backup, file sharing, monitoring, password, and support tools.                                      |
| 4 | Compare total cost including implementation, support, add-ons, internal admin, renewal, and exit.                                    |
| 5 | Review quarterly: reclaim licenses, retire duplicates after migration, and fund lifecycle replacement and contingency.               |

## What to watch for

**WATCH:** A security product is sold without coverage, alert ownership, or reporting.

**WATCH:** Backup is treated as a feature of file sync.

**WATCH:** Every employee receives the most expensive license regardless of role.

**WATCH:** A low monthly price excludes projects, after-hours support, and common requests.

**WATCH:** Core accounts or domains are owned by a vendor instead of the business.

# Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

|                     |                                                              |       |
|---------------------|--------------------------------------------------------------|-------|
| <b>NOW</b>          | Name the owner and confirm the current state.                | _____ |
| <b>NEXT 7 DAYS</b>  | Fix the highest-risk gap or gather the missing evidence.     | _____ |
| <b>NEXT 30 DAYS</b> | Complete the remaining quick wins and set review dates.      | _____ |
| <b>NEXT QUARTER</b> | Test the process, document results, and assign improvements. | _____ |

## Notes / decisions / questions for your provider

---

---

---

---

---

**Want a second set of eyes? Book a free consultation at [brotherlytechnology.com/contact/](https://brotherlytechnology.com/contact/) or call 404-907-1005.**

**Reference points:** CISA Secure Our World: [cisa.gov/secure-our-world](https://cisa.gov/secure-our-world) | NIST Cybersecurity Framework 2.0: [nist.gov/cyberframework](https://nist.gov/cyberframework)

This guide is educational and is not legal, regulatory, tax, or insurance advice. Confirm requirements and pricing for your organization with qualified advisors and vendors.