Small Business Security Baseline Checklist

A practical overview of foundational security controls for small and growing businesses

Summit Cybersecurity & IT Solutions
Reports & Guides • Version 1.0 • February 2026

Why This Checklist Exists

Most security incidents affecting small and growing businesses are not the result of advanced attacks. They occur because foundational controls were missing, outdated, or never reviewed.

This checklist outlines a **baseline set of security practices** that support system stability, reduce operational risk, and improve recovery outcomes. It is not a compliance framework, certification, or audit tool.

Instead, it is intended to help business owners understand *what good looks like* at a foundational level.

How to Use This Checklist

- This checklist is **technology-agnostic**
- Not every item applies to every environment
- Gaps do not indicate failure — they highlight opportunity
- Security maturity improves over time through consistency

The goal is awareness, not perfection.

Identity & Access Management

User Access & Authentication

- ☐ Each individual has a unique user account
- ☐ Administrative access is limited and reviewed
- ☐ Multi-factor authentication is enabled where supported
- ☐ Former employees' access is removed promptly
- ☐ Shared credentials are minimized and documented

Access sprawl is one of the most common sources of avoidable risk.

Devices & System Management

Endpoints, Servers, and Devices

- ☐ All devices are inventoried and accounted for
- ☐ Operating systems are kept up to date
- ☐ Unsupported or end-of-life systems are identified
- ☐ Security protections are enabled on devices
- ☐ Devices follow consistent configuration standards

Devices do not need to be perfect — they need to be visible and maintained.

Updates, Patching & Change Awareness

System Updates & Maintenance

- ☐ Operating system updates are applied regularly
- ☐ Key business applications are patched consistently
- ☐ Update failures are reviewed and addressed
- ☐ Changes are documented, even when minor
- ☐ Updates are not deferred indefinitely

Unpatched systems often function normally until they don't.

SUMMIT
CYBERSECURITY & IT SOLUTIONS

Backup & Recovery Fundamentals

Backup Coverage & Recovery Readiness

- ☐ Critical systems and data are identified
- ☐ Backups run on a defined schedule
- ☐ Backup data is encrypted and protected
- ☐ Retention aligns with business requirements
- ☐ Restore testing is performed periodically

Backups exist to support recovery — not just storage.

Visibility, Ownership & Review

Oversight & Accountability

- ☐ Ownership of systems and security is clearly defined
- ☐ Alerts and reports are reviewed regularly
- ☐ Issues are tracked and resolved intentionally
- ☐ Service provider responsibilities are understood
- ☐ Security posture is reviewed periodically

Security improves when ownership is clear.

Interpreting the Results

Reviewing this checklist provides insight into where foundational controls are in place — and where attention may be needed.

- Gaps indicate **risk exposure**, not failure
- Many issues can be corrected without major disruption
- Consistency matters more than perfection
- Baselines improve predictability and confidence

Establishing a security baseline helps businesses move from reactive fixes to intentional management. This is typically the first step toward long-term stability.