15

Microsoft 365 security checks.

Every small business should know where it stands.

Use this guide with your IT team to review the foundations: identity, devices, information, and recovery. For each check, record the evidence, an owner, and the next action.

How to use this checklist

01 Review each check with an authorized administrator.

02 Mark Reviewed, Action needed, or Needs investigation.

03 Record evidence and an owner for every action.

04 Prioritize changes, test them, and keep a recovery path.

A starting point, not a complete audit or compliance attestation. Features and licensing vary. No checklist can guarantee protection against every incident.

01-05 / Identity & access

01 Know your Global Administrators

List accounts with Global Administrator and other privileged roles. Confirm each role has a current business reason and owner; use narrower roles where possible.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

02 Verify MFA is enforced

Review how MFA is required through security defaults or Conditional Access. Registration alone does not show that all relevant sign-ins are protected.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

03 Review legacy authentication

Identify applications and protocols relying on older authentication. Plan any blocking policy with your IT team and test business-critical dependencies.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

04 Protect emergency access

Document emergency administrator access, protect the accounts, monitor their use, and test the recovery procedure without weakening normal access controls.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

05 Remove stale employee access

Review former employees, inactive users, and role changes. Confirm sessions, application access, and company devices are addressed during offboarding.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

06-10 / Data & devices

06 Review guests and external sharing

Check guest accounts, shared links, Teams, SharePoint, and OneDrive access. Confirm information is only shared with the intended people.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

07 Check application consent

Review enterprise applications, app registrations, and granted permissions. Investigate unnecessary or unrecognized access with an authorized administrator.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

08 Account for every company device

Compare your device inventory with Intune or your management platform. Identify unmanaged, inactive, and personally owned devices accessing business data.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

09 Verify encryption and recovery keys

Check BitLocker or appropriate disk encryption on company laptops. Confirm recovery keys are safely stored and available to authorized staff when needed.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

10 Review device compliance and access

Check device compliance policies and access decisions. Test changes in stages; some controls require additional Microsoft licenses.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

11-15 / Protection & recovery

11 Confirm endpoint protection is healthy

Check Defender or the protection service you use for onboarding, current status, and unresolved alerts. Know who reviews and responds to findings.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

12 Check patching and local admin access

Review update coverage, unsupported operating systems, and local administrator privileges. Assign owners and deadlines to exceptions.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

13 Review email protection

Check anti-phishing settings, suspicious forwarding rules, and mail authentication records. Validate proposed changes before applying them to production mail.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

14 Make logs and alerts useful

Confirm audit and sign-in data are available for the required time period. Route actionable alerts to an accountable person and document the response process.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

15 Test recovery, not just backups

Identify critical information, recovery requirements, and backup coverage. Test an authorized restore and record what worked, what failed, and what needs attention.

☐ Reviewed ☐ Action needed ☐ Investigate

Owner / evidence: _____

Turn findings into action.

Focus on impact, assign ownership, and confirm the result.

Priority 1

Action _____

Owner / target date _____

Evidence / validation _____

Priority 2

Action _____

Owner / target date _____

Evidence / validation _____

Priority 3

Action _____

Owner / target date _____

Evidence / validation _____

Current vendor guidance

Microsoft Entra security defaults

Microsoft Intune device encryption

Microsoft email protection recommendations

Need a closer look?

Explore the ExousiaSec Security Baseline Assessment.