AEGIREN · FREE RESOURCE

Securing Microsoft 365 in a small company

15 checks you can run yourself — no sign-up, no email required

Aegiren — access and identity security **Version** v1.0 **Updated** 16 July 2026 **Sharing** free — pass it on

Who this is for

You run a company of 5 to 80 people on Microsoft 365. You have no in-house IT, or one person already doing everything. You suspect your accounts may not be properly protected, but you don't know where to start looking.

This checklist answers that. Fifteen checks, each with **the exact place to look** in your admin portals, what a healthy setup looks like versus one that needs work, and why it matters.

What you need: an admin account, or an account with the *Global Reader* role, which lets you view everything without changing anything. **Allow one hour.** Following this document changes nothing in your tenant — it only looks.

What this is not: an audit. It covers what actually causes incidents in small organisations, not every Microsoft 365 setting. It replaces neither an independent review nor a prioritised action plan.

Why access, and not something else

The vast majority of small-business breaches don't start with an exotic technical flaw. They start with **an account**: a reused password, a convincing phishing email, a former employee's account nobody disabled, an administrator without multi-factor authentication. The attacker doesn't break in — they sign in.

That's good news: most of the measures below are **free**, already included in your subscription, and take hours rather than weeks.

How to score

Give each check a colour.

- **Green** — the healthy situation described applies to you.
- **Amber** — partially in place, or you're not sure.
- **Red** — the risky situation described is yours.

A red isn't a disaster, it's a task. What matters is knowing which ones you have.

> **A note on portals.** Microsoft renames its screens regularly. The paths below are current; if a label has changed, search for the feature name in the relevant portal's search bar.
>
> `entra.microsoft.com` — Microsoft Entra admin center (identity, access)
> `admin.microsoft.com` — Microsoft 365 admin center (users, licences)
> `security.microsoft.com` — Microsoft Defender portal (security, email)
> `purview.microsoft.com` — Microsoft Purview portal (audit, compliance)

1. Secure Score

The question: Microsoft continuously scores your environment's security posture. What's yours, and have you ever looked at it?

Where to check: Defender portal → *Exposure management* → *Secure Score*.

Why it matters: it's the only free measure Microsoft gives you of your own posture, with recommendations ranked by impact. A low score means the default settings were never tightened — and defaults favour ease of use, not security.

GREEN You know your score, you track it, and the high-impact recommendations have been addressed.
RED You're seeing this screen for the first time, or the score is below 50%.

2. Dormant accounts

The question: how many active accounts haven't signed in for more than ninety days?

Where to check: Entra admin center → *Identity* → *Users* → *All users*, with the last sign-in column displayed. Full sign-in history requires an Entra ID P1 licence; without it, cross-check against your actual headcount.

Why it matters: an unused account is still an open door, and it usually has the oldest password and the fewest protections. An account belonging to someone who left two years ago won't alert anyone if it's used on a Sunday night. You're also paying a licence for each of them.

GREEN No active account without a sign-in in ninety days, and you review this quarterly.
RED You find accounts belonging to people who have left, still active.

3. Administrators

The question: how many people are *Global Administrator* in your tenant?

Where to check: Entra admin center → *Identity* → *Roles and administrators* → *Global Administrator*.

Why it matters: a global administrator can do anything — read any mailbox, reset any password, delete any data. Every such account is a key to the kingdom. It's common to find six or eight in a forty-person company, often because a previous IT provider was never removed.

GREEN Two global administrators at most, one of them a rarely used break-glass account, and administrators use a dedicated account separate from their day-to-day mailbox.

RED More than three global administrators, or admin accounts also used for email and web browsing.

4. Multi-factor authentication

The question: is MFA enforced for **everyone**, and through what mechanism?

Where to check: Entra admin center → *Protection* → *Authentication methods*, then the registration activity tab. Also check whether *Security defaults* are on (Entra → *Identity* → *Overview* → *Properties*).

Why it matters: this is the single best effort-to-protection ratio available. Without a second factor, one stolen password is enough to take over a mailbox — the CEO's, or finance's. Watch for the common trap: MFA enabled "for admins only", or offered without being required.

Not all methods are equal: an authenticator app beats SMS, which remains vulnerable to SIM swapping.

GREEN One hundred percent of accounts, admins first, with an authenticator app as the primary method.
RED Accounts without MFA, or enrolment left to each person's discretion.

5. Conditional access policies

The question: are there rules that allow or block a sign-in based on its context?

Where to check: Entra admin center → *Protection* → *Conditional Access* → *Policies*. Requires an Entra ID P1 licence, included in Business Premium.

Why it matters: without these rules, every sign-in is treated identically — your accountant from the office, and a stranger from the other side of the world at 3 a.m. A baseline is four policies: MFA for everyone, block legacy protocols, stronger protection for administrators, and a response to risky sign-ins.

GREEN A baseline is in place, tested, with a break-glass account excluded so you can't lock yourself out.
RED No policies at all, or only *Security defaults* when your licence allows better.

6. Legacy authentication

The question: can old mail protocols still be used to sign in?

Where to check: Entra admin center → *Monitoring* → *Sign-in logs*, filtered by client app to show legacy authentication clients only. Look at the last thirty days.

Why it matters: these older protocols — POP, IMAP, basic-auth SMTP — **cannot handle multi-factor authentication**. While they remain open they bypass every protection you've put in place, and they are the primary target of automated password-spraying attacks.

GREEN No legacy sign-ins over thirty days, with an explicit block in place.
RED Legacy sign-ins appear in the logs, or you've never checked.

7. Mail forwarding and anti-phishing

The question: can a user automatically forward all their email to an outside address? And is your anti-phishing protection configured?

Where to check: Defender portal → *Policies & rules* → *Threat policies* → *Anti-spam outbound policy* for automatic forwarding, and *Anti-phishing* for protection. Also review mailbox rules in the Exchange admin center.

Why it matters: a quiet forwarding rule is **the classic signature of a compromised mailbox**. An attacker who gains access creates a rule that copies everything to them, then steps back: they keep reading without ever signing in again. This is the core mechanism behind invoice and payment fraud.

GREEN Automatic external forwarding is blocked, and anti-phishing protection is strengthened for executives and finance.
RED External forwarding is unrestricted, or you find forwarding rules nobody knowingly created.

---

8. External file sharing

The question: who can receive a link to your documents, and do those links expire?

Where to check: SharePoint admin center → *Policies* → *Sharing*.

Why it matters: the most permissive setting produces links that work **for anyone who holds them, with no authentication at all**. Forwarded, found in a compromised mailbox, or simply forgotten in an old email, such a link stays valid indefinitely. Many organisations discover hundreds of live anonymous links nobody remembers creating.

GREEN Sharing is limited to authenticated people, links expire, and sensitive shares have been reviewed.
RED "Anyone" sharing is allowed, with no expiry.

---

9. Offboarding

The question: when someone leaves, what exactly happens, and who does it?

Where to check: nowhere — this is the one item on the list that isn't on a screen. Take the last person who left and inspect their account.

Why it matters: weeks often pass between someone's last day and their account actually being disabled. And disabling isn't enough: until **active sessions are revoked**, access from an already-signed-in personal phone can continue. A written procedure covers blocking sign-in, revoking sessions, resetting the password, deciding what happens to the mailbox, and transferring documents.

GREEN A written procedure exists, is applied on the day of departure, and the last leaver's account was handled correctly.
RED Nothing written down, or you find former employees' accounts still active.

---

10. The audit log

The question: is unified audit logging switched on, and how long is history retained?

Where to check: Purview portal → *Audit*. If the screen offers to start recording, it's off.

Why it matters: this is your black box. Without it, after an incident it is **impossible** to know which files were opened, which emails were read, or since when. You can't size the damage, answer your insurer, or notify a data breach properly. Turning it on takes minutes, costs nothing, and has no user impact — but it isn't retroactive: whatever wasn't recorded is gone.

GREEN Logging is on, and you know the retention period your licences provide.
RED Logging is off, or you don't know.

---

11. Passwords and self-service reset

The question: can a user reset their own password securely? And do you still force periodic changes?

Where to check: Entra admin center → *Protection* → *Password reset*, and *Authentication methods* → *Password protection* for the banned-terms list.

Why it matters: two ideas have changed. First, properly configured self-service reset with two verification methods is **safer** than a call to support where someone recognises the caller's voice — that call is exactly what social engineering exploits. Second, forced expiry every ninety days is now **advised against** by Microsoft and by national security agencies alike: it mechanically produces `Spring2026!` followed by `Summer2026!`. A long, unique password that never expires, paired with MFA, protects considerably better.

GREEN Self-service reset is enabled with two verification methods, passwords no longer expire, and obvious terms tied to your company are banned.
RED No self-service reset, or forced expiry still in force.

---

12. Backup

The question: if all your email and files were deleted or encrypted today, how would you recover them six months from now?

Where to check: find out whether a third-party backup solution is in place. This is not a native Microsoft 365 feature: if nobody can name the tool, there isn't one.

Why it matters: this is the costliest misunderstanding in cloud computing. Microsoft guarantees the **availability of its platform**, not the **recovery of your content** from your own incidents — that's the shared responsibility model, written into your service terms. What you have is not a backup but a **recycle bin with limited retention**, roughly thirty to ninety-three days depending on the item. It recovers a file deleted last week; it restores nothing three months after a disaster. And modern ransomware encrypts precisely the files **synchronised** to OneDrive and SharePoint.

GREEN A third-party backup covers Exchange, OneDrive, SharePoint and Teams with a defined retention period — and **a restore has actually been tested**.
RED No third-party backup, or a backup nobody has ever tested restoring from.

---

13. Devices

The question: can company data be reached from unmanaged personal devices?

Where to check: Intune admin center → *Devices* → *Compliance*. Without an Intune licence the question still stands: which phones and laptops actually hold your email?

Why it matters: an unencrypted, unpatched family computer shared with teenagers can today sync an entire document library. If it's lost or stolen, without disk encryption and a screen lock, the data is readable directly.

GREEN Minimum compliance rules — encryption, screen lock, up-to-date OS — gate access to company data.
RED Any device can connect and sync, no conditions attached.

---

14. External guests

The question: how many outside people have access to your tenant, and since when?

Where to check: Entra admin center → *Identity* → *Users*, filtered by user type *Guest*.

Why it matters: every contractor, accountant, intern or partner invited into a Teams space stays there. The engagement ends; the invitation doesn't. It's common to find several dozen guests in a fifty-person company, many of them now working elsewhere — and a guest's access sits entirely outside your security controls, since it depends on how well *their* account is protected.

GREEN The guest list is known, justified, and reviewed at least twice a year.
RED The number surprises you, or you find guests from long-finished engagements.

---

15. Risky sign-ins

The question: what happens when Microsoft detects a suspicious sign-in — from an unusual country, an anonymised address, or with a password known from a public breach?

Where to check: Entra admin center → *Protection* → *Identity Protection* → *Risky users* and *Risky sign-ins*. Automated policies require an Entra ID P2 licence; viewing detections does not.

Why it matters: Microsoft does the detecting for you. Without an associated policy, the detection lands on a screen nobody opens, and nothing happens. With one, a risky sign-in automatically triggers an MFA challenge or a forced password change — a response in the middle of the night, with no human involved.

GREEN Detections are reviewed, and automated policies respond to high risk.
RED Nobody has ever opened that screen.

So what now?

Count your colours.

Five reds or more. This is common and no cause for panic: it mostly means your settings are still the ones you started with. Begin with items 4, 3, 6 and 12 — MFA, the number of administrators, legacy protocols, and backup. Those four close most of the real risk, and the first three are free.

One to four reds. Your foundation holds. Work through them in the order they appear above: the list is ordered by decreasing impact.

No reds, a few ambers. You're above average for your size. The subject then becomes consistency — a quarterly review of accounts, guests and shares — rather than configuration.

One honest closing note. This list tells you *where* you stand. It doesn't tell you what, in your specific situation, deserves attention first, or what each fix actually costs. That work — looking, comparing against a benchmark, scoring, prioritising — is exactly what I do for companies your size: a few hours spread over two weeks, fully remote, delivered in writing.

If you'd like to talk it through, or simply ask about one item on this list: **contact@aegiren.com**. Asking a question commits you to nothing.

Benchmarks. This checklist draws on the *CIS Microsoft 365 Foundations Benchmark* and the French national cybersecurity agency's (ANSSI) IT hygiene guide, adapted to the reality of a 5-to-80-seat organisation.

Aegiren — Your Microsoft 365, audited, hardened, documented.
Written by Mithra · v1 · 2026 · aegiren.com