FREE GUIDE

10 Microsoft 365 settings every small business should check

A practical checklist for Microsoft 365 tenants used by small businesses and charities. Written in plain English, with where to click and what "good" looks like.

These are the settings we look at first when we are asked to review a Microsoft 365 tenant. They do not replace a full security assessment, but if you put them in good order you will have closed many of the gaps that still catch small organisations out. Menus are those in the Microsoft 365, Entra, Defender, Purview and SharePoint admin centres as they stood in November 2026; names do move around, so use the search box in each admin centre if a path has changed.

1 Multi-factor authentication and security defaults

WHY IT MATTERS

A stolen or guessed password is still one of the most common ways a mailbox or a tenant is taken over. Multi-factor authentication (MFA) asks for a second proof of identity, which stops the great majority of password-only attacks.

WHERE TO FIND IT

In the Microsoft Entra admin centre (entra.microsoft.com), go to Entra ID > Overview > Properties, then choose Manage security defaults. You can also reach identity settings from the Microsoft 365 admin centre (admin.microsoft.com) under Show all > Identity. If you already use Conditional Access, manage MFA there instead (see setting 4).

WHAT GOOD LOOKS LIKE

For a small tenant that does not yet use Conditional Access, security defaults should be on, and every user should have registered MFA — preferably an authenticator app rather than text messages alone. Microsoft turns security

defaults on for most new tenants, but older tenants, or ones where it was switched off “to stop the prompts”, are often unprotected. Do not turn security defaults off unless you have replaced them with equivalent Conditional Access policies. If security defaults and Conditional Access are both off, that is an urgent gap.

2 Block legacy authentication

WHY IT MATTERS

Older email protocols such as basic authentication for POP, IMAP, SMTP AUTH and some ActiveSync clients cannot enforce MFA. Attackers still try these “legacy” sign-in methods because a password on its own may be enough.

WHERE TO FIND IT

If security defaults are enabled, legacy authentication is already blocked. If you use Conditional Access, open the Microsoft Entra admin centre > Entra ID > Conditional Access and create or review a policy that applies to all users, with Conditions > Client apps including Exchange ActiveSync and Other clients, and Grant set to Block access. Also review the Exchange admin centre for any mailboxes that still have SMTP AUTH enabled.

WHAT GOOD LOOKS LIKE

Legacy authentication is blocked for everyone, with any exception documented, named and temporary. Microsoft has already retired basic authentication for many Exchange Online protocols; do not re-enable it. After the block is in place, check the Entra sign-in logs for failed legacy attempts so you can see whether an old phone or a line-of-business app still needs a modern alternative.

3 Limit Global Administrators and use emergency access accounts

WHY IT MATTERS

The Global Administrator role can change every setting, read almost any mailbox and grant any other role. The more people who have it, the larger the impact if one of those accounts is phished. At the other extreme, a single admin and no backup can lock you out of your own tenant.

WHERE TO FIND IT

In the Microsoft Entra admin centre, go to Entra ID > Roles & admins and open Global Administrator to see who is assigned. Review other directory roles in the

same place, and give people the least privileged role that lets them do their job (for example Exchange Administrator, SharePoint Administrator or Helpdesk Administrator).

WHAT GOOD LOOKS LIKE

Microsoft recommends at least two, and fewer than five, Global Administrators for day-to-day use. Everyday work should use narrower roles. In addition, create two cloud-only emergency (or "break-glass") accounts that use the organisation's onmicrosoft.com domain and are not synchronised from on-premises systems. Microsoft now recommends phishing-resistant methods such as FIDO2 security keys for these accounts. Exclude them only from Conditional Access policies that could prevent an emergency sign-in, store the keys or credentials securely, do not use the accounts for ordinary work, turn on sign-in alerts, and test them on a regular schedule.

4 Conditional Access

WHY IT MATTERS

Security defaults are a strong starting point, but they are all-or-nothing. Conditional Access lets you require MFA for everyone, apply stricter rules to administrators, block risky or legacy sign-ins, and ask for a compliant or Microsoft Entra joined device when that is appropriate.

WHERE TO FIND IT

Microsoft Entra admin centre > Entra ID > Conditional Access (sometimes listed under Protection). Conditional Access needs Microsoft Entra ID P1, which is included with Microsoft 365 Business Premium and Microsoft 365 E3, and is available as an add-on to some other plans. It is not included with Business Basic or Business Standard alone.

WHAT GOOD LOOKS LIKE

Security defaults are off only because Conditional Access is on and enforced. Start with Microsoft's baseline templates: require MFA for all users, require MFA for administrators and for Azure management, and block legacy authentication. Use report-only mode to test a policy before you enforce it. Exclude emergency access accounts with care, and keep a written note of why each exclusion exists. Named locations can help, but an office IP address is not a substitute for MFA.

5 Disable automatic external email forwarding

WHY IT MATTERS

Once an attacker has access to a mailbox, they often add a forwarding rule so that copies of new mail — including invoices, password resets and customer conversations — continue to leave the organisation quietly. The same setting is sometimes turned on by accident when someone is on leave.

WHERE TO FIND IT

In the Microsoft Defender portal (security.microsoft.com), go to Email & collaboration > Policies & rules > Threat policies > Anti-spam, then open the anti-spam outbound policy and find Automatic forwarding. Also check the Exchange admin centre > Recipients > Mailboxes for mailbox-level forwarding, and look for inbox rules that send mail outside the organisation.

WHAT GOOD LOOKS LIKE

Automatic forwarding to external addresses is set to Off — Forwarding is disabled, for the whole tenant. Do not leave the option on "Automatic — System-controlled", because that behaves differently in different tenants. If someone has a genuine need to forward mail outside, treat it as a documented exception and review it. After a staff member leaves, confirm that no forwarding or inbox rules remain.

6 External sharing in SharePoint and OneDrive

WHY IT MATTERS

A sharing link that works for "anyone with the link" can outlive the project it was created for, be forwarded to the wrong person, or be discovered later. Guests and former contractors are another common source of leftover access.

WHERE TO FIND IT

Open the SharePoint admin centre from the Microsoft 365 admin centre (Show all > SharePoint), then go to Policies > Sharing. The same page covers OneDrive; OneDrive can be more restrictive than SharePoint, but not more open. Review individual sites under Sites > Active sites if a particular team needs a tighter or looser exception.

WHAT GOOD LOOKS LIKE

The organisation-wide setting is not "Anyone" unless you have a clear, current reason for anonymous links. "New and existing guests" is a typical baseline for a

small business that works with clients or suppliers. Set the default link type to "Specific people", add an expiry on guest or anonymous links if you allow them, and periodically review existing "Anyone" links and guest accounts. When someone leaves, remove their account and any guest access they sponsored.

7 Turn on audit logging

WHY IT MATTERS

If a mailbox is compromised, a file disappears, or an app is granted permission it should not have, you need a record of what happened. Audit logs cannot be recreated for a period when logging was off.

WHERE TO FIND IT

Sign in to the Microsoft Purview portal (purview.microsoft.com) and open Audit. If you see a banner asking you to start recording user and admin activity, turn it on. Auditing is on by default for many enterprise plans, but not for Microsoft 365 Business Basic, Business Standard or Business Premium — on those plans you must enable it yourself.

WHAT GOOD LOOKS LIKE

Unified audit logging is on, and someone in the business knows how to search it (or who to ask). Standard audit typically retains records for 180 days, depending on your licences. Leave it on. If you handle more sensitive work, ask about longer retention or Audit (Premium), which needs a higher licence.

8 Anti-phishing and Microsoft Defender policies

WHY IT MATTERS

A convincing message that looks as if it came from a supplier, a director or Microsoft itself is still the usual starting point for fraud and ransomware. The built-in email filters help, but they need to be switched on and, where you are licensed for it, extended with Safe Links and Safe Attachments.

WHERE TO FIND IT

In the Microsoft Defender portal, go to Email & collaboration > Policies & rules > Threat policies. The most straightforward approach is to apply the Standard or Strict preset security policies. You can also review the individual Anti-phishing, Anti-spam and Anti-malware policies, plus Safe Links and Safe Attachments. Safe

Links and Safe Attachments are part of Microsoft Defender for Office 365, which is included with Microsoft 365 Business Premium and some higher plans, or as an add-on — they are not included with Business Basic or Business Standard alone.

WHAT GOOD LOOKS LIKE

The Standard (or Strict) preset is applied to all users, or you have custom policies that achieve the same outcome. Anti-phishing impersonation protection covers your own domains and senior people. If you are licensed for Defender for Office 365, Safe Links and Safe Attachments are on. Staff have a simple way to report a suspicious message, and you have looked at Microsoft Secure Score as a trend, not as a target of 100 at any cost.

9 Restrict user consent to applications

WHY IT MATTERS

A well-written "Allow access" prompt can persuade someone to grant a third-party app permission to read mail, files or contacts. That is a common way for attackers to stay in a tenant without knowing a password.

WHERE TO FIND IT

In the Microsoft Entra admin centre, go to Entra ID > Enterprise applications > Consent and permissions > User consent settings. It is also wise to set Entra ID > Users > User settings > Users can register applications to No, unless you have a reason to allow it. Under Consent and permissions > Admin consent settings you can let staff request approval instead of granting access themselves.

WHAT GOOD LOOKS LIKE

User consent is set to "Do not allow user consent", or at most to "Allow user consent for apps from verified publishers, for selected permissions". An administrator reviews requests. Existing enterprise applications are reviewed, and anything you do not recognise is investigated and removed. This is one of the highest-value changes you can make in an afternoon.

10 Backup, retention and recovery

WHY IT MATTERS

Microsoft 365 keeps deleted items for a time, and retention policies can preserve records, but that is not the same as a separate backup. Ransomware, a malicious or

accidental deletion, or a misunderstood retention setting can still cause lasting loss — and Microsoft's shared responsibility model leaves recovery planning with you.

WHERE TO FIND IT

Check deleted-item recovery in Outlook and in the Exchange admin centre, and the SharePoint and OneDrive recycle bins (the second-stage recycle bin is in the SharePoint admin centre). Retention policies live in the Microsoft Purview portal under Data lifecycle management. Exchange deleted-item retention is 14 days by default and can be extended to 30. If you need a full backup, look at Microsoft 365 Backup or a specialist Microsoft 365 backup service; the right choice depends on how quickly you need to restore and what you must be able to recover.

WHAT GOOD LOOKS LIKE

You know, in writing, how long mail and files can be recovered after deletion, and you have tested that this works. A retention policy matches your legal and business needs rather than keeping everything for ever. For information you cannot afford to lose, there is a backup that is separate from the live tenant, and you have practised a restore. Do not assume that "it is in Microsoft 365, so it is already backed up".

Also worth checking: self-service password reset

Self-service password reset (SSPR) lets people unblock their own account instead of waiting for an administrator. You will find it in the Microsoft Entra admin centre under Entra ID > Protection > Password reset. Enabling it for all users typically needs Microsoft Entra ID P1 (included with Business Premium). Require more than one authentication method, and combine registration with MFA so people are not asked twice. It is a close cousin of setting 1, which is why it sits just outside this list of ten.

This guide is for typical small-business and charity Microsoft 365 tenants and was written in November 2026. What you can turn on depends on your licences, and Microsoft updates both the product and the admin centres. It is practical guidance, not a complete security audit, and not legal advice. If you would like Cloud Team 247 to review your tenant, please book a Microsoft 365 Security Check.

Cloud Team 247 is the trading name of Red Team 247 Limited, 4 Clews Road, B98 7ST. Telephone 01214235960.