# Microsoft 365 Security Checklist

Ten configuration checks every Microsoft 365 business should run.

EMERGING IT

The items below cover the configuration gaps we see most regularly in Microsoft 365 environments. Work through each one and note any that flag for your setup. If you need help interpreting what you find, reply to the email and we'll introduce you to one of our security consultants.

01 ☐

## MFA enforcement method

Confirm you're using Conditional Access policies, not Security Defaults. Security Defaults apply MFA broadly but can't be scoped by user, location, or device and leave gaps in legacy authentication scenarios. Conditional Access requires a higher licence tier but closes those gaps.

02 ☐

## Legacy authentication blocked

Protocols such as SMTP Auth, IMAP, and POP3 bypass MFA entirely. These should be blocked via Conditional Access or Entra ID unless there is a specific, documented business reason to keep them active. Most businesses have no legitimate need for them.

03 ☐

## Admin accounts restricted to admin tasks

Accounts with Global Admin or other privileged roles should not be used for email or day-to-day work. Each administrator should have a separate standard user account for daily activity. Using a privileged account for routine tasks is one of the most common exposures we see.

04 ☐

## Shared mailbox access controls

Shared mailboxes should have no active password and should only be accessible via delegated access from named, individually authenticated accounts. Direct login to shared mailboxes is frequently overlooked and creates an authentication bypass.

05 ☐

## Email forwarding rules audit

Any user with mailbox access can create a rule that silently copies or forwards email to an external address. Review both Exchange transport rules and per-mailbox forwarding settings. Rules created by an attacker during a compromise will remain active after the password is reset.

06 ☐

## Unified audit logging enabled

Audit logging is not enabled by default on all Microsoft 365 plans. Confirm the unified audit log is active and that retention periods meet your incident response or compliance requirements. Without it, you have no record of what happened if a breach occurs.

07 ☐

## External sharing settings reviewed

SharePoint and OneDrive are often configured with 'Anyone with a link' sharing enabled by default. This allows files to be shared outside the organisation without authentication. Set external sharing to the minimum required for your business and review any links already in circulation.

08 ☐

## Privileged role assignments reviewed

Review who holds Global Admin, Exchange Admin, SharePoint Admin, and other privileged roles. Permanent role assignments should be limited to the minimum number of accounts necessary. Where possible, use Privileged Identity Management (PIM) to require just-in-time elevation.

09 ☐

## Microsoft Secure Score reviewed

Secure Score gives a point-in-time view of your Microsoft 365 configuration against Microsoft's own security recommendations. A score below 50 typically indicates several high-impact items are unaddressed. Use it as a baseline, not a compliance standard.

10 ☐

## Incident response path confirmed

If a breach occurs, you need a clear escalation path before you need it. Confirm your IT provider or internal team has a documented incident response procedure, that admin contact details in the Microsoft 365 tenant are current, and that someone outside the tenant can access it if credentials are compromised.