MICROSOFT 365 SECURITY CHECKLIST

BEST PRACTICES FOR A SECURE TENANT

3rd Element Consulting

Why This Matters

A Microsoft 365 tenant has hundreds of individually configurable security settings, spread across identity, email, sharing, devices, and data protection, and none of it is set once and left alone. Microsoft changes the platform constantly: new features ship, defaults shift, and a setting that was fine last year isn't automatically still fine today.

This isn't a project to take on yourself. It's a way to check whether whoever manages your Microsoft 365 environment today has actually covered this ground.

Work through each section and ask your IT provider directly: is this in place, and how do you know? If the answer is vague, or nobody's checked in a while, that's worth knowing.

LICENSING

- ☐ Business Basic and Business Standard do not include Conditional Access on their own. Conditional Access requires Entra ID P1, which is only bundled with Business Premium, or purchased separately as an add-on.
- ☐ Business Premium is the starting point for a secure tenant, unless Entra ID P1 (or an equivalent third-party SSO and Conditional Access solution) is added on top of Basic or Standard.
- ☐ Defender for Business, Intune, and Purview DLP all travel with Business Premium. If staying on a lower tier plus add-ons, confirm equivalent coverage actually exists for each of these, not just Conditional Access.

IDENTITY & SIGN-IN SECURITY

- ☐ Multi-factor authentication is enforced for every user, not just admins.
- ☐ Legacy authentication protocols (which can't support MFA) are disabled tenant-wide.
- ☐ Conditional access policies govern sign-in based on location, device, and risk level.
- ☐ Admin accounts are separate from everyday user accounts, and use privileged role assignment rather than standing admin rights.
- ☐ A regular access review confirms former employees and contractors no longer have active accounts.

EMAIL SECURITY

- ☐ Anti-phishing and impersonation protection policies are configured, not left on default settings.
- ☐ External sender warnings are enabled so users can see when a message originates outside the organization.
- ☐ SPF, DKIM, and DMARC are all configured correctly for your domain.
- ☐ Mailbox forwarding rules are monitored, since silent auto-forwarding is a common sign of a compromised account.
- ☐ Anti-malware and safe attachment scanning are enabled for incoming mail.

SHARING & COLLABORATION (TEAMS, SHAREPOINT, ONEDRIVE)

- ☐ External sharing defaults are intentional, not left wide open by default.
- ☐ Shared links have expiration dates, particularly for sensitive files.
- ☐ Guest access is reviewed periodically, not granted once and forgotten.
- ☐ Sensitive files are labeled so sharing and DLP rules can actually act on them.

DATA PROTECTION

- ☐ Sensitivity labels are applied to classify and protect sensitive content.
- ☐ Data loss prevention (DLP) policies are configured to flag or block sensitive data leaving the organization.
- ☐ Retention policies are set for mailboxes, Teams, and SharePoint so data isn't kept indefinitely by default or deleted before it should be.

DEVICE & APPLICATION ACCESS

- ☐ Mobile device and app management policies control what happens to company data on personal devices.
- ☐ Third-party app consent is reviewed and restricted, since a user-approved app can quietly gain broad access to company data.
- ☐ Legacy protocols and unmanaged devices are blocked from accessing the tenant.

ADMIN & AUDIT

- ☐ Unified audit logging is turned on so activity across the tenant can actually be reviewed.
- ☐ Admin role assignments are reviewed periodically, not granted once during setup and left alone.
- ☐ A break-glass emergency access account exists in case of an identity provider outage or lockout.

BACKUP

- ☐ An independent backup of mailboxes, OneDrive, SharePoint, and Teams exists, separate from Microsoft's own retention and recycle bin features.
- ☐ Backups are tested with real restores, not just confirmed to be running.

AI & COPILOT READINESS

- ☐ Sharing and permissions have been reviewed and cleaned up before enabling Copilot tenant-wide.
- ☐ Sensitive files are properly labeled so Copilot doesn't surface them to someone who shouldn't see them.

- ☐ There's a clear inventory of what AI tools are already connected to the tenant today.

Want a second opinion on your Microsoft 365 environment?

Schedule an IT Environment Review