CORPORATE
DATA SOLUTIONS INC.

Microsoft 365 Security Checklist

The 5 Most Commonly Missed Configurations

Most organizations use Microsoft 365 but don't configure it securely. Use this checklist to assess your environment across the five areas where we most commonly find gaps.

☐ MFA required for ALL user accounts (not just admins)
☐ MFA method documented and tested (authenticator app preferred, SMS acceptable)
☐ Grace period for MFA enforcement set (users have X days to enroll)
☐ Legacy authentication blocked (SMTP, POP3, IMAP with password disabled)

Status: ☐ All Met ☐ Partially Met ☐ Not Started

☐ Block access from unusual locations (impossible travel detection)
☐ Require MFA for risky sign-in activity (new device, unusual IP)
☐ Block or require MFA for unmanaged devices accessing email/Teams
☐ Require MFA for all admin accounts (no exceptions)

Status: ☐ All Met ☐ Partially Met ☐ Not Started

☐ Global admin count minimized (fewer than 3 people)
☐ Dedicated admin accounts for admin work (not used for daily email/Teams)
☐ Privileged access management in place (admin actions logged and reviewed)
☐ Service accounts restricted (if used, strongly authenticated)

Status: ☐ All Met ☐ Partially Met ☐ Not Started

☐ Advanced threat protection enabled (malware, phishing, zero-day detection)
☐ Spam filtering configured (not too aggressive, not too permissive)
☐ External email warning enabled (users see banner on outside messages)
☐ DLP policies in place for sensitive data (PII, financial, IP)

Status: ☐ All Met ☐ Partially Met ☐ Not Started

☐ SharePoint permissions audited (no over-sharing of sensitive sites)
☐ External sharing controlled (specific domains allowed, not everyone)

☐ Teams guest access policies in place (who can invite externals)
☐ Sensitive site protection enabled (deleted sites retained, audit logging)

Status: ☐ All Met ☐ Partially Met ☐ Not Started

Count your "All Met" sections:

5/5 sections: Excellent. You're configured better than 80% of organizations.
3-4 sections: Good foundation. Gaps exist but attackers need to work harder.
1-2 sections: Significant gaps. Email-based attacks will likely succeed.
0 sections: High risk. Configuration is default/neglected. Act immediately.

Questions? Not sure how to interpret this? CDSI offers complimentary 15-minute M365 security audits.

Phone: (480) 366-4567
Email: sales@cdsi.support