

CHECKLIST · TOMORIS TOOLBOX

Securing Microsoft 365: Checklist for Entra ID, Exchange, SharePoint, and Teams

Key settings for Entra ID, Exchange Online, Defender, SharePoint, OneDrive, and Teams, with CISA baseline identifiers and licensing notes

UPDATED

Oct 25, 2026

LENGTH

PDF, 9 pages

ONLINE

tomoris.com/en/downloads/microsoft-365-sicherheitscheckliste

AT A GLANCE

2 to 8

Global Administrators according to CISA SCuBA

30 days

Maximum validity of "Anyone" links according to CISA

6

Services at a glance, from Entra ID to Teams

v2.0.0

Version of the CISA baselines (ScubaGear)

WHO IT IS FOR

- Microsoft 365 administrators in small and medium-sized companies
- IT service providers that manage Microsoft 365 tenants for customers
- Information security officers who review the state of a tenant

WHAT THIS COVERS

This checklist summarizes the most important security settings for Microsoft 365 per service: Entra ID, Exchange Online, protection against malware and phishing, SharePoint and OneDrive, Teams, and logs. It is based on the baselines of the US agency CISA from the SCuBA project (ScubaGear v2.0.0 of October 22, 2026) and on Microsoft's documentation. Each item names the baseline identifier so that you can look it up and check it with the free ScubaGear tool.

This checklist is a TOMORIS recommendation based on the CISA baselines, which are binding only for US federal agencies. Microsoft's names, default values, and license terms change constantly; Microsoft's current documentation and the currently valid version of the baselines are authoritative. Test changes before implementing them, for example with emergency access and a pilot group.

CONTENTS

01	How to use the checklist	2
02	Microsoft Entra ID: sign-in and accounts	3
03	Microsoft Entra ID: roles, apps, and guests	4
04	Exchange Online: email and mailboxes	5
05	Protection against malware and phishing	5
06	SharePoint and OneDrive: sharing	6
07	Microsoft Teams: meetings and external contacts	7
08	Logs, alerts, and measurement	7
09	Licensing notes	8
10	Sources	9

01 —

How to use the checklist

Where the items come from, what "shall" and "should" mean, and how you measure

In the SCuBA project, CISA publishes secure baseline configurations for Microsoft 365. For US federal agencies, the mandatory requirements (SHALL) are binding through BOD 25-01; CISA makes the baselines available to other organizations as a reference. The baselines assume at least a Microsoft 365 E3 license and only name licenses that go beyond it. With ScubaGear, CISA provides a free tool that checks a tenant against the baselines. Items from the baselines show the identifier, such as MS.AAD.1.1, and whether the baseline requires the item (shall) or recommends it (should); items without an identifier come from Microsoft Learn or are TOMORIS recommendations.

Microsoft Secure Score	Microsoft Secure Score measures the security posture; a higher number means more recommendations implemented. It is available in the Microsoft Defender portal.
Security defaults	For tenants on the free tier of Entra ID: MFA registration for everyone, MFA for administrators and, when needed, for all users, blocking of legacy protocols and the device code flow, protection of privileged activities.
Conditional Access	With Entra ID P1 or P2, Conditional Access policies are usually the better choice than security defaults, according to Microsoft.

This checklist is a TOMORIS recommendation based on the CISA baselines; not every item suits every company. Test changes in advance so that you do not lock anyone out. Multifactor authentication and Conditional Access are covered in detail in the separate checklist "Introducing MFA in Microsoft 365", and SPF, DKIM, and DMARC in the email security guide.

02

Microsoft Entra ID: sign-in and accounts

Block legacy protocols, strong sign-in, emergency access

Microsoft recommends blocking sign-ins with legacy protocols because they do not support multifactor authentication. According to Microsoft's analysis, more than 97% of credential stuffing attacks and more than 99% of password spray attacks use such protocols.

- ☐ Legacy authentication blocked (MS.AAD.1.1, shall).
- ☐ Phishing-resistant MFA for all users (MS.AAD.3.1, shall), such as device-bound passkeys, FIDO2 security keys, Windows Hello for Business, or certificate-based authentication; as a minimum, MFA for all users, for example as long as phishing-resistant methods are not yet possible (MS.AAD.3.2, shall); always phishing-resistant for highly privileged roles (MS.AAD.3.6, shall).
- ☐ SMS, voice call, and email one-time passcode disabled as methods (MS.AAD.3.5, shall); sign-in context shown in Microsoft Authenticator (MS.AAD.3.3, shall).
- ☐ Device code sign-in blocked (MS.AAD.3.9, should).
- ☐ High-risk users and high-risk sign-ins blocked (MS.AAD.2.1 and 2.3, shall; requires Entra ID P2).
- ☐ Passwords do not expire (MS.AAD.6.1, shall); details in the password policy.
- ☐ At least two emergency access accounts, cloud-only with a *.onmicrosoft.com domain, not synchronized, protected with a passkey (FIDO2) or certificate (Microsoft Learn).

- ☐ Without a license for Conditional Access: security defaults enabled (Microsoft Learn).

03 —

Microsoft Entra ID: roles, apps, and guests

Few Global Administrators, restricted app consent, controlled guests

- ☐ Two to eight people with the Global Administrator role (MS.AAD.7.1, shall); Microsoft recommends fewer than five, CISA allows additional accounts, for example for emergency access.
- ☐ Finer-grained roles instead of Global Administrator for administrative tasks (MS.AAD.7.2, shall).
- ☐ Privileged accounts cloud-only, separate from on-premises Active Directory (MS.AAD.7.3, shall).
- ☐ No permanently active assignments of highly privileged roles, Global Administrator activation only with approval, alerts on assignment and activation (MS.AAD.7.4 to 7.8, shall; alert for other highly privileged roles 7.9, should; Entra ID P2 or another PAM solution).
- ☐ Only administrators register applications (MS.AAD.5.1, shall).
- ☐ User consent for applications restricted (MS.AAD.5.2, shall); Microsoft recommends allowing it at most for apps from verified publishers.
- ☐ Admin consent workflow configured (MS.AAD.5.3, shall).
- ☐ Guests with restricted access to directory objects (MS.AAD.8.1, should); only people with the Guest Inviter role may invite (MS.AAD.8.2, should), only to approved domains (MS.AAD.8.3, should).
- ☐ New in v2.0.0: risky AI agents blocked (MS.AAD.9.1, shall; according to CISA with Entra ID P2 and Microsoft Agent 365 or Microsoft 365 E7).

As a baseline list of highly privileged roles, to be extended with further roles as needed, CISA names: Global Administrator, Privileged Role Administrator, User Administrator, SharePoint Administrator, Exchange Administrator, Hybrid Identity Administrator, Application Administrator, and Cloud Application Administrator.

04 —

Exchange Online: email and mailboxes

Forwarding, sender protection, SMTP AUTH, sharing, and auditing

- ☐ Automatic forwarding to external domains disabled (MS.EXO.1.1, shall): CISA implements this through the remote domain "Default", for which automatic forwarding is not allowed. In addition, select "Off – Forwarding is disabled" in the outbound spam policy: the default value "Automatic – System-controlled" behaves differently depending on the tenant.
- ☐ SPF rejecting unauthorized senders, DKIM for all domains, DMARC with p=reject (MS.EXO.2.2, 4.1, 4.2, shall; DKIM MS.EXO.3.1, should).
- ☐ SMTP AUTH disabled organization-wide (MS.EXO.5.1, shall); allowed as an exception only for individual mailboxes that demonstrably need it. If security defaults are active, SMTP AUTH is already disabled.
- ☐ Contact and calendar details not shared with all domains (MS.EXO.6.1 and 6.2, shall).
- ☐ External sender warning for messages enabled (MS.EXO.7.1, shall).
- ☐ Mailbox auditing active (MS.EXO.13.1, shall); according to Microsoft enabled by default in all organizations, but check it anyway.

If automatic forwarding is disabled, user inbox rules and administrator forwarding that redirect messages to external addresses also stop working; the sender receives a non-delivery report (Microsoft Learn).

05 —

Protection against malware and phishing

Preset policies, attachments, links, impersonation, and exceptions

With the Standard and Strict preset security policies, Microsoft applies recommended settings for email protection; they are practically not configurable. The Built-in protection preset policy gives users without another assignment baseline protection through Safe Attachments and Safe Links from Defender for Office 365.

- ☐ Standard preset security policy assigned to most users, Strict to selected, particularly at-risk accounts (Microsoft Learn).
- ☐ Attachments that can be executed with a click blocked, at least .exe, .cmd, and .vbe (MS.SECURITYSUITE.1.1, shall).
- ☐ Emails also scanned after delivery, malware quarantined or dropped (MS.SECURITYSUITE.1.2 and 1.3, shall).

- ☐ Attachments in SharePoint, OneDrive, and Teams scanned for malware (MS.SECURITYSUITE.1.4, should).
- ☐ Impersonation protection for particularly at-risk accounts, your own domains, and important suppliers and partners (MS.SECURITYSUITE.2.1 to 2.3, should; Defender for Office 365).
- ☐ Spam and phishing not delivered to the inbox, no allowed domains in anti-spam protection (MS.SECURITYSUITE.6.1 and 6.2, shall).
- ☐ Links in emails, Teams, and Office documents checked against blocklists, clicks logged (MS.SECURITYSUITE.7.1 and 7.3, should; Defender for Office 365).
- ☐ No IP allow lists and no safe lists (MS.SECURITYSUITE.8.1 and 8.2, should).
- ☐ Data loss prevention policy configured for your sensitive data types (MS.SECURITYSUITE.3.1, shall; 3.2 to 3.5, should).

06 —

SharePoint and OneDrive: sharing

Limit external sharing, secure default links, expiration for "Anyone" links

Levels of external sharing (Microsoft Learn), from open to closed

Anyone	Links that let anyone access files or folders without signing in.
New and existing guests	Invited people sign in with their account or verify their identity with a code.
Existing guests	Sharing only with guests who are already in the directory.
Only people in your organization	External sharing is turned off.

- ☐ External sharing for SharePoint and OneDrive limited to "Existing guests" or "Only people in your organization" (MS.SHAREPOINT.1.1 and 1.2, shall), or set more openly in a deliberate and documented way.
- ☐ External sharing restricted to approved domains or security groups (MS.SHAREPOINT.1.3, shall).
- ☐ Default link "Specific people" with view permissions (MS.SHAREPOINT.2.1 and 2.2, shall).
- ☐ Where "Anyone" links are allowed: expiration after at most 30 days, view permissions only (MS.SHAREPOINT.3.1 and 3.2, shall).
- ☐ Guests using a verification code sign in again after at most 30 days (MS.SHAREPOINT.3.3, shall).

07 —

Microsoft Teams: meetings and external contacts

Who may start meetings, join them, and make contact

According to Microsoft, all external domains are allowed by default for external access in Teams. With an allow list, you restrict chats and meetings to the organizations you actually work with; all other domains are then blocked.

- ☐ External access only for approved domains (MS.TEAMS.2.1, shall).
- ☐ Unmanaged Teams accounts cannot contact internal users (MS.TEAMS.2.2, shall); internal users do not contact them on their own initiative (MS.TEAMS.2.3, should).
- ☐ Anonymous users cannot start meetings (MS.TEAMS.1.2, shall); anonymous participants and dial-in users wait in the lobby (MS.TEAMS.1.3 and 1.5, should).
- ☐ External participants cannot request control of shared screens (MS.TEAMS.1.1, should).
- ☐ Meeting recording according to your own rules; CISA recommends disabling it (MS.TEAMS.1.6, should).
- ☐ Teams email integration disabled (MS.TEAMS.4.1, shall).
- ☐ Only approved Microsoft, third-party, and custom apps can be installed (MS.TEAMS.5.1 to 5.3, should).

08 —

Logs, alerts, and measurement

Turn on auditing, forward alerts, measure progress

Caution with Business plans: According to Microsoft, audit logging is not enabled by default for Microsoft 365 Business Basic, Business Standard, and Business Premium and must be turned on manually.

- ☐ Unified audit log enabled (MS.SECURITYSUITE.5.1, shall) and status checked in the Microsoft Purview portal.
- ☐ Logs searchable for at least 3 months and retrievable for 12 months (MS.SECURITYSUITE.5.2, shall); according to CISA, longer than 180 days in Microsoft 365 requires E5, Microsoft Purview Suite, or the E5 eDiscovery and Audit add-on.
- ☐ Security alerts enabled and sent to a monitored mailbox or a SIEM (MS.SECURITYSUITE.4.1, shall; 4.2, should).

- ☐ Entra ID sign-in and audit logs forwarded to the team that evaluates security events (MS.AAD.4.1, shall).
- ☐ Microsoft Secure Score recorded as a baseline and reviewed regularly.
- ☐ ScubaGear assessment carried out and deviations documented with reasons.

09

Licensing notes

Which items need more than Microsoft 365 E3 according to CISA

Additional licenses according to CISA SCuBA v2.0.0 (assumption: at least E3)

FEATURE	LICENSE ACCORDING TO SOURCE	IDENTIFIER
Risk-based policies	Microsoft Entra ID P2	MS.AAD.2
Managed devices for sign-in and MFA registration	Microsoft Intune	MS.AAD.3.7, 3.8
Just-in-time role activation, approval, alerts	Microsoft Entra ID P2 or another PAM solution	MS.AAD.7.4 to 7.9
Block risky AI agents	Entra ID P2 and Microsoft Agent 365 or Microsoft 365 E7	MS.AAD.9.1
Safe Attachments, Safe Links, impersonation protection	Defender for Office 365 Plan 1 or 2 (included in E5, add-on for E3)	MS.SECURITYSUITE.1.3, 1.4, 2, 7
Data loss prevention in Teams and on devices	E5 or a comparable third-party solution	MS.SECURITYSUITE.3, 3.5
Custom audit retention policy	E5 or E3 with compliance add-on	MS.SECURITYSUITE.5
Audit retention beyond 180 days	E5, Microsoft Purview Suite, or E5 eDiscovery and Audit add-on	MS.SECURITYSUITE.5
Send Entra logs to an external system	Possibly an Azure subscription	MS.AAD.4.1

Which of these features are included in your plan, such as Microsoft 365 Business Premium, is stated in Microsoft's service descriptions; check this before implementation. Prices and license bundles change constantly and are not part of this checklist.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

Microsoft 365 domain check (German)

tomoris.com/tools/microsoft-365-check

Email security check (German)

tomoris.com/tools/email-security-check

DMARC generator

tomoris.com/en/tools/dmarc-generator

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

10

Sources

All statements are supported by sources. Legislation applies in its current version.

- 1 **CISA SCuBA baseline Microsoft Entra ID (ScubaGear v2.0.0, October 22, 2026)**
MS.AAD.1 to 9, list of highly privileged roles, license requirements, accessed October 25, 2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- 2 **CISA SCuBA baseline Exchange Online (v2.0.0)**
MS.EXO.1 to 7 and 13, accessed October 25, 2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- 3 **CISA SCuBA baseline Security Suite (v2.0.0)**
MS.SECURITYSUITE.1 to 8, license requirements, accessed October 25, 2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- 4 **CISA SCuBA baseline SharePoint and OneDrive (v2.0.0)**
MS.SHAREPOINT.1 to 3, accessed October 25, 2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- 5 **CISA SCuBA baseline Microsoft Teams (v2.0.0)**
MS.TEAMS.1, 2, 4, 5, accessed October 25, 2026
github.com/cisagov/ScubaGear/blob/v2.0.0/PowerShell/ScubaGear/b...
- 6 **CISA: Secure Cloud Business Applications (SCuBA) Project**
Project, ScubaGear as a free assessment tool, accessed October 25, 2026
www.cisa.gov/resources-tools/services/secure-cloud-business-app...
- 7 **Microsoft Learn: Microsoft Secure Score**
Introduction, accessed October 25, 2026
learn.microsoft.com/de-de/defender-xdr/microsoft-secure-score
- 8 **Microsoft Learn: Security defaults in Microsoft Entra ID**
Content, target audience, Conditional Access with P1/P2, accessed October 25, 2026
learn.microsoft.com/de-de/entra/fundamentals/security-defaults
- 9 **Microsoft Learn: Block legacy authentication**
Overview, accessed October 25, 2026
learn.microsoft.com/de-de/entra/identity/conditional-access/pol...
- 10 **Microsoft Learn: Emergency access accounts**
Number, cloud accounts, authentication, accessed October 25, 2026
learn.microsoft.com/de-de/entra/identity/role-based-access-cont...
- 11 **Microsoft Learn: Automatic external email forwarding**
Three settings and their effect, accessed October 25, 2026
learn.microsoft.com/de-de/defender-office-365/outbound-spam-pol...
- 12 **Microsoft Learn: Turn auditing on (Microsoft Purview)**
Default status, exception for Business plans, accessed October 25, 2026
learn.microsoft.com/de-de/purview/audit-log-enable-disable
- 13 **Microsoft Learn: Best practices for Microsoft Entra roles**
No. 5, fewer than five Global Administrators, accessed October 25, 2026
learn.microsoft.com/de-de/entra/identity/role-based-access-cont...
- 14 **Microsoft Learn: User consent for applications**
Recommendation of verified publishers, accessed October 25, 2026
learn.microsoft.com/de-de/entra/identity/enterprise-apps/config...
- 15 **Microsoft Learn: Preset security policies**
Standard, Strict, Built-in protection, accessed October 25, 2026
learn.microsoft.com/de-de/defender-office-365/preset-security-p...
- 16 **Microsoft Learn: Enable or disable SMTP AUTH**
Organization and mailbox setting, accessed October 25, 2026
learn.microsoft.com/de-de/exchange/clients-and-mobile-in-exchan...
- 17 **Microsoft Learn: Mailbox auditing**
Enabled by default, accessed October 25, 2026
learn.microsoft.com/de-de/purview/audit-mailboxes
- 18 **Microsoft Learn: External sharing in SharePoint and OneDrive**
Sharing levels, accessed October 25, 2026
learn.microsoft.com/de-de/sharepoint/turn-external-sharing-on-o...
- 19 **Microsoft Learn: External access in Microsoft Teams**
Default: all external domains, allow list, accessed October 25, 2026
learn.microsoft.com/de-de/microsoftteams/trusted-organizations-...