

CHECKLISTE · MICROSOFT 365

Microsoft 365 absichern – Baseline für KMU

Priorisierte Einstellungen für Identität, Administratoren, E-Mail, Freigaben, Geräte und Protokollierung.

DAS ERHALTEN SIE

- Security Defaults vs. Conditional Access – was passt?
- Schutz von Admin-Konten inkl. Notfallzugang
- E-Mail-Schutz: SPF, DKIM, DMARC, Defender
- Freigaben, Geräte, Audit – mit Lizenzhinweisen

AUF EINEN BLICK

Für	**Administratoren und IT-Verantwortliche**
Zeitbedarf	**ca. 1 Tag Prüfung, Umsetzung schrittweise**
Stand	**16. November 2026**
Version	**2.0**

Unverbindliche Praxishilfe – keine Rechtsberatung, kein Audit

1 Vorab: Lizenzumfang klären

> Schützen Sie zuerst Identitäten und privilegierte Zugänge. Ergänzen Sie danach E-Mail-, Daten-, Geräte- und Überwachungskontrollen.

Viele Funktionen hängen vom gebuchten Plan ab. Prüfen Sie vor der Umsetzung, welche Lizenzen tatsächlich zugewiesen sind. Die Tabelle zeigt typische Zuordnungen – maßgeblich ist die aktuelle Microsoft-Dokumentation.

Funktion	Typischerweise enthalten in
Security Defaults (Basis-MFA)	Allen Microsoft-365-Tenants ohne Zusatzkosten
Conditional Access (bedingter Zugriff)	Microsoft Entra ID P1, z. B. in Microsoft 365 Business Premium
Privileged Identity Management (PIM)	Microsoft Entra ID P2 bzw. entsprechende Pakete
Defender for Office 365 (Sichere Links/Anlagen)	Plan 1 z. B. in Business Premium; Plan 2 in E5-Paketen
Intune (Geräteverwaltung)	Z. B. Business Premium, E3/E5

Bevor Sie Richtlinien aktivieren

Legen Sie zwei Notfallzugänge (Break-Glass-Konten) an, testen Sie neue Richtlinien zunächst im Berichtsmodus bzw. mit einer Pilotgruppe und informieren Sie die Mitarbeitenden. Eine falsch konfigurierte Richtlinie kann alle Benutzer – auch Administratoren – aussperren.

2 Identität und Anmeldung

Option	Wann sinnvoll	Hinweis
Security Defaults	Kleine Tenants ohne Entra ID P1	MFA für alle, Blockieren veralteter Authentifizierung – einfach, aber nicht anpassbar
Conditional Access	Ab Entra ID P1 (z. B. Business Premium)	Feingranular nach Benutzer, Gerät, Standort, Risiko; Security Defaults dann deaktivieren

Empfohlene Basis-Richtlinien (Conditional Access)

- MFA für alle Benutzer; für Administratoren phishing-resistente Methoden (FIDO2-Sicherheitsschlüssel, Passkeys, Windows Hello for Business).
- Veraltete Authentifizierungsprotokolle blockieren.
- Zugriff auf Unternehmensdaten nur von konformen bzw. verwalteten Geräten (wo Intune genutzt wird).
- Anmeldungen aus nicht benötigten Ländern einschränken – mit Ausnahme der Notfallkonten.
- In Microsoft Authenticator Nummernabgleich und Kontextinformationen nutzen; SMS nur als Übergangslösung.

Self-Service-Kennwortzurücksetzung

Aktivieren Sie die Kennwortzurücksetzung mit MFA-Methoden, damit Benutzer nicht auf unsichere Wege (Telefonanruf beim Helpdesk ohne Prüfung) ausweichen.

3 Administratoren schützen

- Separate Admin-Konten ohne Postfach und ohne Alltagsnutzung; keine Admin-Rechte für das persönliche Konto.
- Rolle „Globaler Administrator“ nur für wenige Personen (Microsoft empfiehlt weniger als fünf); sonst spezifische Rollen (z. B. Exchange-, Benutzer-, Helpdesk-Administrator).
- Mit PIM (sofern lizenziert): Rollen nur zeitlich begrenzt und mit Begründung aktivieren (Just-in-Time).
- Admin-Anmeldungen ausschließlich mit phishing-resistenter MFA und von vertrauenswürdigen Geräten.
- Partner- und Dienstleisterzugänge (GDAP) regelmäßig prüfen und auf das Nötige beschränken.

Notfallzugang (Break-Glass)

Anforderung	Umsetzung
Zwei Konten	Cloud-only-Konten, nicht an Personen gebunden
Starke Anmeldung	Phishing-resistente MFA, z. B. FIDO2-Schlüssel, sicher verwahrt
Ausnahme	Von Richtlinien ausgenommen, die alle sperren könnten – aber überwacht
Alarm	Jede Anmeldung mit diesen Konten löst eine Benachrichtigung aus
Test	Funktion regelmäßig (z. B. halbjährlich) prüfen und dokumentieren

4 E-Mail-Schutz

Maßnahme	Zweck
SPF	Legt fest, welche Server im Namen Ihrer Domain senden dürfen
DKIM	Signiert ausgehende E-Mails kryptografisch – für jede eigene Domain aktivieren
DMARC	Richtlinie für nicht authentifizierte E-Mails; von *p=none* mit Berichten schrittweise zu *quarantine* bzw. *reject*
Voreingestellte Sicherheitsrichtlinien	Standard- oder Strikt-Profil für Anti-Spam, Anti-Malware, Anti-Phishing (EOP/Defender)
Sichere Links / Anlagen	Prüfung von Links und Anhängen zum Klickzeitpunkt (Defender for Office 365)
Automatische Weiterleitung nach extern	Standardmäßig blockieren; Ausnahmen begründet freigeben

Maßnahme	Zweck
Kennzeichnung externer Absender	Hinweis in E-Mails von außerhalb der Organisation

5 Freigaben, Geräte und Protokollierung

SharePoint, OneDrive, Teams

- „Jeder mit dem Link" deaktivieren oder mit Ablaufdatum versehen
- Standard-Linktyp: „Personen in Ihrer Organisation"
- Gastzugriffe regelmäßig überprüfen
- Externe Freigabe je Website nach Bedarf

Geräte (Intune)

- Konformitätsrichtlinien: Verschlüsselung, Updates, Bildschirmsperre
- BitLocker auf Windows-Geräten
- Windows LAPS für lokale Admin-Kennwörter
- Mobile Apps mit App-Schutzrichtlinien

Protokollierung

- Einheitliches Überwachungsprotokoll (Microsoft Purview Audit) aktiv?
- Aufbewahrungsdauer Ihres Plans prüfen
- Warnungen für verdächtige Weiterleitungsregeln und Admin-Änderungen
- Anmeldeprotokolle regelmäßig auswerten

Kontinuierlich verbessern

- Microsoft Secure Score als Orientierung – nicht als Ziel an sich
- Neue Funktionen und Standardänderungen verfolgen
- Konfiguration dokumentieren und versionieren
- Quartalsweise Review

Datensicherung

Aufbewahrungsrichtlinien und Papierkorb ersetzen keine Sicherung. Prüfen Sie eine separate Microsoft-365-Sicherung (siehe KONTORIT Wissen „Backup-Strategie 3-2-1").

6 Checkliste

	Prüfpunkt	Verantwortlich	Termin / Nachweis
IDENTITÄT			
☐	Lizenzumfang ist dokumentiert.	_____	_____
☐	Zwei Break-Glass-Konten existieren, sind überwacht und getestet.	_____	_____
☐	MFA ist für alle Benutzer aktiv (Security Defaults oder Conditional Access).	_____	_____
☐	Veraltete Authentifizierung ist blockiert.	_____	_____
☐	Admins nutzen phishing-resistente MFA.	_____	_____
ADMINISTRATION			
☐	Admin-Konten sind getrennt, ohne Postfach.	_____	_____
☐	Weniger als fünf globale Administratoren.	_____	_____
☐	Partner-/Dienstleisterzugänge sind geprüft.	_____	_____
E-MAIL, DATEN, GERÄTE			
☐	SPF, DKIM und DMARC sind für alle Domains eingerichtet.	_____	_____
☐	Voreingestellte Sicherheitsrichtlinien sind aktiv.	_____	_____
☐	Externe Auto-Weiterleitung ist blockiert.	_____	_____
☐	„Jeder mit dem Link“ ist eingeschränkt.	_____	_____
☐	Geräte sind verschlüsselt und verwaltet.	_____	_____
☐	Audit-Protokoll ist aktiv, Warnungen sind eingerichtet.	_____	_____

Quellen & weiterführende Referenzen

- Microsoft Learn: Sicherheitsstandards (Security Defaults) in Microsoft Entra ID
- Microsoft Learn: Conditional Access – allgemeine Richtlinienvorlagen; Notfallzugriffskonten verwalten
- Microsoft Learn: Privileged Identity Management; Empfehlungen zu Administratorrollen
- Microsoft Learn: SPF, DKIM und DMARC in Microsoft 365; voreingestellte Sicherheitsrichtlinien in EOP und Defender for Office 365
- Microsoft Learn: Microsoft Purview Audit; Microsoft Secure Score
- CIS Microsoft 365 Foundations Benchmark, cisecurity.org
- BSI IT-Grundschutz-Kompendium, Bausteine zu Cloud-Nutzung und Office-Produkten, bsi.bund.de

---

Unterstützung gewünscht? KONTORIT begleitet kleine und mittlere Unternehmen in Hamburg bei Bestandsaufnahme, Umsetzung und Betrieb. Anfrage: **kontorit.de/kontakt** · E-Mail: **support@kontorit.de**

Dieses Dokument ist eine allgemeine, unverbindliche Orientierungshilfe. Es ersetzt keine individuelle Beratung, kein Sicherheitsaudit, keine Rechts- oder Steuerberatung und keinen Zertifizierungsnachweis. Produktfunktionen, Lizenzen und rechtliche Anforderungen ändern sich; prüfen Sie den aktuellen Stand anhand der genannten Quellen und Ihrer konkreten Umgebung. Genannte Marken gehören ihren jeweiligen Inhabern. © 2026 KONTORIT · Stand 16. November 2026 · Version 2.0