

VORLAGE · TOMORIS TOOLBOX

Passwortrichtlinie: Vorlage nach NIST und BSI

Richtlinientext mit Platzhaltern, alte und neue Regeln mit Fundstelle und Checkliste für Microsoft Entra ID, belegt mit NIST SP 800-63B-4, BSI ORP.4 und Microsoft Learn

STAND

25.10.2026

UMFANG

PDF, 11 Seiten

ONLINE

tomoris.com/downloads/passwortrichtlinie-vorlage

AUF EINEN BLICK

15

Zeichen Mindestlänge ohne MFA (NIST SP 800-63B-4)

64

Zeichen Höchstlänge mindestens zulassen (NIST)

Kein Ablauf MFA

Wechsel nur bei Verdacht (NIST); NIS2: Abstand festlegen

Pflicht für Admin-Portale von Microsoft, im NISG genannt

FÜR WEN

- Geschäftsführung kleiner und mittlerer Unternehmen, die eine verbindliche Passwortrichtlinie erlassen wollen
- IT-Leitung und Informationssicherheitsbeauftragte, die bestehende Regeln auf den Stand von NIST und BSI bringen
- IT-Dienstleister, die Passwortregeln und Microsoft Entra ID für ihre Kunden einrichten

WURUM ES GEHT

Viele Passwortrichtlinien verlangen noch Sonderzeichen und einen Wechsel alle 90 Tage. Die aktuelle NIST SP 800-63B-4 vom Juli 2025 untersagt beides für Anmeldesysteme und setzt auf Länge, Sperrlisten und begrenzte Fehlversuche; das BSI rät im IT-Grundschutz von rein zeitgesteuerten Wechseln ab. Diese Vorlage übersetzt die Anforderungen in einen Richtlinientext mit Platzhaltern, stellt alte und neue Regeln mit Fundstelle gegenüber und führt durch die Umsetzung in Microsoft Entra ID.

Diese Vorlage ist an Ihr Unternehmen, Ihre Systeme und Ihren Schutzbedarf anzupassen und ersetzt keine Rechtsberatung. Maßgeblich sind die genannten Standards und Herstellerangaben in der jeweils aktuellen Fassung, für Einrichtungen unter dem NISG 2026 der Gesetzestext in der geltenden Fassung. Funktionen, Bezeichnungen und Lizenzen von Microsoft können sich ändern.

INHALT

01	Was NIST und BSI heute verlangen	2
02	Alte Regel, neue Regel	3
03	Wo Mehr-Faktor-Authentisierung Pflicht ist	4
04	Vorlage: Passwortrichtlinie zum Anpassen	5
05	Umsetzung in Microsoft Entra ID	7
06	Vorgaben für Anmeldesysteme und eigene Anwendungen	8
07	Häufige Fehler bei der Umstellung	9
08	Ausblick: Passkeys statt Passwörter	9
09	In vier Schritten zur neuen Richtlinie	10
10	Quellen	10

01

Was NIST und BSI heute verlangen

Die neuen Grundregeln auf einen Blick und wie verbindlich die Quellen für Unternehmen in Österreich sind.

Die US-Standardisierungsbehörde NIST hat im Juli 2025 die SP 800-63B-4 als endgültige Fassung veröffentlicht; sie ersetzt die bisherige SP 800-63B. Sie richtet sich an Informationssysteme der US-Regierung und ist für Unternehmen in Österreich nicht verbindlich, eignet sich aber als Maßstab. SHALL bedeutet verpflichtend, SHOULD empfohlen. Für Anmeldesysteme gilt unter anderem: mindestens 15 Zeichen, wenn das Passwort der einzige Faktor ist, keine Regeln zu Zeichenarten, kein Wechsel nach Frist, eine Sperrliste und höchstens 100 Fehlversuche (3.1.1.2, 3.2.2).

Das IT-Grundschutz-Kompendium des deutschen BSI (Edition 2023) verlangt, den Passwortgebrauch verbindlich zu regeln (ORP.4.A8). Rein zeitgesteuerte Wechsel SOLLTEN vermieden werden; dafür MÜSSEN Maßnahmen ergriffen werden, um kompromittierte Passwörter zu erkennen (ORP.4.A23). Basis-Anforderungen

sind vorrangig zu erfüllen, Standard-Anforderungen bilden mit ihnen den Stand der Technik. Auf seiner Verbraucherseite empfiehlt das BSI lange Passwörter, etwa fünf bis sechs zufällig gewählte Wörter mit Leerzeichen, nennt daneben kürzere Passwörter mit vier Zeichenarten und rät zum Passwortmanager.

Pflicht oder Empfehlung? NIST und IT-Grundschutz sind Standards, keine Gesetze in Österreich. Gesetzlich genannt ist Multi-Faktor-Authentifizierung für wesentliche und wichtige Einrichtungen in § 32 Abs. 4 lit. j NISG 2026; für sie gelten außerdem die Anforderungen an die Authentifizierung im Anhang der Durchführungsverordnung (EU) 2024/2690 (§ 2 NISV 2026), siehe Abschnitt 02. Die Vorlage in diesem Dokument ist eine Empfehlung von TOMORIS auf Grundlage dieser Quellen.

02

Alte Regel, neue Regel

Neun verbreitete Passwortregeln und was nach NIST SP 800-63B-4 und BSI ORP.4 an ihre Stelle tritt.

Gegenüberstellung mit Fundstelle (NIST = SP 800-63B-4, ORP.4 = BSI IT-Grundschutz Edition 2023)

BISHER ÜBLICH	NEU	FUNDSTELLE
Mindestens 8 Zeichen mit Groß- und Kleinbuchstaben, Ziffer und Sonderzeichen	Länge statt Zeichenarten: mindestens 15 Zeichen, mindestens 8 nur zusammen mit MFA; keine weiteren Zusammensetzungsregeln	NIST 3.1.1.2; Microsoft empfiehlt für Microsoft 365 mindestens 14 Zeichen
Wechsel alle 30, 60 oder 90 Tage	Kein Wechsel nach Frist; Pflichtwechsel bei Verdacht oder Hinweis auf Kompromittierung	NIST 3.1.1.2; ORP.4.A8, ORP.4.A23
Höchstlänge 12 oder 16 Zeichen, Leerzeichen verboten	Mindestens 64 Zeichen zulassen, alle druckbaren Zeichen und Leerzeichen; die volle Länge prüfen	NIST 3.1.1.2; ORP.4.A23
Keine Prüfung gegen bekannte Passwörter	Sperrliste häufiger, erwartbarer und kompromittierter Passwörter; Ablehnung mit Begründung	NIST 3.1.1.2; ORP.4.A8
Einfügen gesperrt, Passwortmanager unerwünscht	Passwortmanager und automatisches Ausfüllen zulassen, Einfügen erlauben	NIST 3.1.1.2; ORP.4.A8 (Nutzung prüfen)
Sicherheitsfrage und Merkhilfe für das Zurücksetzen	Keine Sicherheitsfragen, keine ohne Anmeldung sichtbaren Merkhilfen; sicheres Rücksetzverfahren	NIST 3.1.1.2; ORP.4.A11
Beliebig viele Anmeldeversuche	Fehlversuche begrenzen: steigende Verzögerung und Sperre ab festgelegter Zahl, höchstens 100	NIST 3.2.2; ORP.4.A13
Passwort als einziger Schutz, auch für Administratoren	MFA, mindestens für Administratoren; ein phishingresistentes Verfahren anbieten	ORP.4.A10, ORP.4.A21; NIST 2.2.2; § 32 Abs. 4 lit. j NISG 2026
Passwörter im Klartext oder umkehrbar verschlüsselt gespeichert	Gesalzen und mit einem Passwort-Hashverfahren gespeichert	NIST 3.1.1.2; ORP.4.A12, ORP.4.A23

NIS2-Einrichtungen: Nach Anhang Nr. 11.6.2 der Durchführungsverordnung (EU) 2024/2690, den § 2 NISV 2026 für anwendbar erklärt, sind Authentifizierungsdaten zu Beginn, in vorab festgelegten Zeitabständen und bei Verdacht zu ändern (lit. c), nach einer festgelegten Zahl erfolgloser Anmeldeversuche das Zurücksetzen der Authentifizierungsdaten und die Sperrung zu verlangen (lit. d), inaktive Sitzungen zu beenden (lit. e) und für privilegierte Konten gesonderte Zugangsdaten zu nutzen (lit. f). Den Zeitabstand legen Sie selbst fest und begründen ihn mit der Risikoanalyse; einen Mindestwert nennt der Anhang nicht.

03

Wo Mehr-Faktor-Authentisierung Pflicht ist

NISG 2026 für NIS2-Einrichtungen und Microsoft für Verwaltungszugänge; das BSI empfiehlt sie (SOLLTE) für Administratoren.

Für wesentliche und wichtige Einrichtungen zählt § 32 Abs. 4 lit. j NISG 2026 seit 1. Oktober 2026 die „Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung“ zu den Mindestinhalten der Risikomanagementmaßnahmen. Sie müssen geeignet und verhältnismäßig sein (Abs. 1 und 3). Näheres regelt die NISV 2026 (BGBl. II Nr. 290/2026): Ihr § 2 erstreckt den Anhang der Durchführungsverordnung (EU) 2024/2690 auf alle wesentlichen und wichtigen Einrichtungen, die die Verordnung nicht schon selbst erfasst. Danach sind Nutzer, soweit angemessen und je nach Klassifizierung der Werte, mit mehreren Faktoren oder kontinuierlich zu authentifizieren (Anhang Nr. 11.7.1).

Microsoft verlangt MFA für Verwaltungszugänge, eine Abwahl ist nicht möglich



Okt. 2024

Admin-Portale

Azure-Portal, Microsoft Entra Admin Center und Intune Admin Center: MFA für jede Verwaltungsaktion, schrittweise in allen Mandanten.



Feb. 2025

Microsoft 365 Admin Center

Schrittweise Durchsetzung der MFA bei der Anmeldung am Microsoft 365 Admin Center.



1. Okt. 2025

Werkzeuge und Schnittstellen

Azure CLI, Azure PowerShell, Azure-App, IaC-Werkzeuge und REST-API für Anlegen, Ändern und Löschen; ein Aufschub war bis 1. Juli 2026 möglich.

Die Microsoft-Pflicht gilt für alle Benutzerkonten, auch für Notfallkonten; für diese empfiehlt Microsoft Passkey (FIDO2) oder zertifikatbasierte Authentifizierung. Verwaltete Identitäten und Dienstprinzipale sind nicht betroffen, Benutzerkonten, die als Dienstkonto Skripte ausführen, schon. Im IT-Grundschutz SOLLTEN Kennungen mit weitreichenden Berechtigungen mit Mehr-Faktor-Authentisierung geschützt werden (ORP.4.A10), bei erhöhtem Schutzbedarf generell (ORP.4.A21). NIST verlangt auf der Stufe AAL2, mindestens ein phishingresistentes Verfahren anzubieten (2.2.2).

Empfehlung von TOMORIS: MFA für alle Konten, mindestens für E-Mail, Cloud-Dienste, Fernzugriff und Administration. Das geht über die hier genannten Pflichten hinaus.

04 —

Vorlage: Passwortrichtlinie zum Anpassen

Mustertext mit 15 Klauseln für alle Konten, besondere Konten und IT-Systeme, dazu die Freigabe zum Ausfüllen.

So passen Sie die Vorlage an: Ersetzen Sie alle Angaben in eckigen Klammern, wählen Sie bei Varianten mit | eine aus und streichen Sie, was nicht zutrifft. Zahlen wie [15] Zeichen sind Vorschläge von TOMORIS auf Grundlage der Quellen. Fundstellen in runden Klammern zeigen, worauf eine Regel beruht; Regeln ohne Fundstelle sind organisatorische Ergänzungen von TOMORIS.

1. Zweck und Geltungsbereich

Diese Richtlinie regelt Wahl, Nutzung, Wechsel und Prüfung von Passwörtern bei der [Unternehmen]. Sie gilt für alle Mitarbeitenden und externen Dienstleister mit Zugang zu ihren Systemen und für alle Benutzer-, Administrator-, Dienst- und Notfallkonten. Verantwortlich ist [Name, Funktion] (ORP.4.A8).

2. Länge statt Zeichenregeln

Passwörter haben mindestens [15] Zeichen; Systeme lassen mindestens [64] Zeichen, alle druckbaren Zeichen und Leerzeichen zu. Vorgaben zu Zeichenarten entfallen, soweit das System es erlaubt. Empfohlen sind Passphrasen aus fünf bis sechs zufälligen Wörtern oder Passwörter aus dem Passwortmanager. Umlaute und ß vermeiden Sie, weil nicht jedes System sie annimmt (NIST 3.1.1.2; BSI).

3. Verbotene Passwörter

Unzulässig sind leicht zu erratende Passwörter, Passwörter aus Listen häufiger oder bekannt gewordener Passwörter und solche mit eigenem Namen, Benutzernamen oder Firmen-, Produkt- und Standortnamen. Systeme prüfen neue Passwörter, soweit möglich, gegen eine Sperrliste und nennen den Ablehnungsgrund (ORP.4.A8; NIST 3.1.1.2).

4. Ein Passwort je Zugang

Jedes Passwort gilt nur für ein System oder eine Anwendung und wird nie für private oder fremde Dienste verwendet. Passwörter sind geheim, nur der Person selbst bekannt und werden unbeobachtet eingegeben (ORP.4.A8; Microsoft-Empfehlungen für Microsoft 365).

5. Passwortmanager

[Produkt] ist als Passwortmanager freigegeben; sein Hauptpasswort ist besonders stark und nur dort im Einsatz. Automatisches Ausfüllen und Einfügen sind erlaubt. Außerhalb davon werden Passwörter nicht schriftlich festgehalten, außer zur Notfallhinterlegung (Ziffer 10). Synchronisierung über Onlinedienste Dritter: [deaktiviert, Pflicht nach ORP.4.A8 | nach dokumentierter Risikoabwägung zugelassen, Abweichung von ORP.4.A8] (ORP.4.A8; NIST 3.1.1.2; BSI).

6. Wechsel nur mit Anlass

Passwörter laufen nicht nach Fristen ab. Ein Passwort wird sofort geändert, wenn es Unbefugten bekannt geworden ist oder der Verdacht besteht; bei Hinweisen auf eine Kompromittierung erzwingt die IT den Wechsel. Einen Verdacht melden Sie umgehend an [Kontakt]. Zur Erkennung kompromittierter Passwörter nutzt die IT [Verfahren]. [Für NIS2-Einrichtungen: Zusätzlich wird alle [Zeitabstand] gewechselt.] (ORP.4.A8, ORP.4.A23; NIST 3.1.1.2; Anhang Nr. 11.6.2 lit. c DVO 2024/2690)

7. Mehr-Faktor-Authentisierung	Für [alle Konten E-Mail, Cloud-Dienste, Fernzugriff und Administration] ist ein zweiter Faktor verpflichtend. Zugelassen sind [Passkey (FIDO2), Sicherheitsschlüssel, Authenticator-App]; phishingresistente Verfahren wie Passkeys werden bevorzugt (ORP.4.A10, ORP.4.A21; NIST 2.2.2; für NIS2-Einrichtungen § 32 Abs. 4 lit. j NISG 2026).
8. Zurücksetzen ohne Sicherheitsfragen	Es gibt keine Sicherheitsfragen und keine Merkhilfen, die ohne Anmeldung sichtbar sind. Vergessene Passwörter werden über [Self-Service mit zweitem Faktor Identitätsprüfung durch den Helpdesk] zurückgesetzt; wer zurücksetzen darf, ist dafür geschult (NIST 3.1.1.2; ORP.4.A11).
9. Administratorkonten	Konten mit weitreichenden Berechtigungen sind einer Person zugeordnet und immer mit MFA geschützt, bevorzugt mit Passkey (FIDO2), Sicherheitsschlüssel oder Zertifikat; gemeinsam genutzte Administratorkennungen sind unzulässig. [Bei erhöhtem Schutzbedarf: Vier-Augen-Prinzip.] (ORP.4.A1, A10, A14, A24)
10. Notfallkonten	Die [Anzahl] Notfallkonten sind mit [Passkey (FIDO2) Zertifikat] geschützt; ihre Zugangsdaten liegen [versiegelt, Ort], nur dafür ist eine schriftliche Hinterlegung erlaubt. Zugriff haben [Name, Funktion] und [Name, Funktion]. Jede Nutzung wird dokumentiert, danach werden die Zugangsdaten gewechselt (ORP.4.A8; Microsoft-Pflicht-MFA).
11. Dienst- und technische Konten	Dienstkonten erhalten zufällig erzeugte Passwörter mit mindestens [Länge] Zeichen, verwaltet in [Produkt]. Automatisierung in Azure nutzt verwaltete Identitäten oder Dienstprinzipale statt Benutzerkonten. Passwortwechsel werden mit [Anwendungsverantwortliche] abgestimmt (ORP.4.A23; NIST 3.1.1.2; Microsoft).
12. Standardpasswörter	Voreingestellte Passwörter und vordefinierte Kennungen werden vor dem produktiven Einsatz geändert, Standardpasswörter durch Passwörter nach dieser Richtlinie ersetzt (ORP.4.A9, ORP.4.A23).
13. Anforderungen an IT-Systeme	Systeme prüfen das vollständige Passwort, sperren nach [10] Fehlversuchen für mindestens [60] Sekunden mit steigender Dauer, verraten nicht, ob Kennung oder Passwort falsch war, lassen alte Passwörter nicht wieder zu, beenden inaktive Sitzungen nach [Minuten], [für NIS2-Einrichtungen: sperren nach [Zahl] Fehlversuchen das Konto und verlangen ein neues Passwort,] übertragen nur verschlüsselt und speichern gesalzen mit einem Passwort-Hashverfahren (NIST 3.1.1.2, 3.2.2; ORP.4.A13, A23; Anhang Nr. 11.6.2 lit. d und e DVO 2024/2690).
14. Einweisung, Ausnahmen, Kontrolle	Alle Mitarbeitenden werden bei Eintritt und [jährlich] eingewiesen (ORP.4.A19). Ausnahmen genehmigt [Name, Funktion] schriftlich, begründet und befristet; die Umsetzung prüft [Name, Funktion] [jährlich].
15. Inkrafttreten	Die Richtlinie gilt ab [Datum], ersetzt [bisherige Regelung] und wird [jährlich] sowie bei Änderungen der zugrunde liegenden Standards überprüft.

Freigabe und Eckdaten zum Ausfüllen

ANGABE	EINTRAG
Unternehmen	_____
Verantwortlich für die Richtlinie (Name, Funktion)	_____
Passwortmanager und zugelassene MFA-Verfahren	_____
Meldestelle bei Verdacht (Kontakt)	_____
Gültig ab, nächste Überprüfung	_____
Freigabe Geschäftsführung (Name, Datum, Unterschrift)	_____

05

Umsetzung in Microsoft Entra ID

Was fest vorgegeben ist, was Sie einstellen können und welche Lizenz Sie dafür brauchen.

Für Konten, die direkt in Entra ID angelegt und verwaltet werden, gilt eine feste Kennwortrichtlinie: 8 bis 256 Zeichen, drei von vier Zeichenarten (Klein- und Großbuchstaben, Ziffern, Symbole), keine Unicode-Zeichen. Ändern lässt sich nur der Ablauf. Für Konten, die aus dem lokalen Active Directory synchronisiert werden, gilt sie nur, wenn die Cloud-Kennwortrichtlinie für synchronisierte Benutzer ausdrücklich aktiviert ist.

Eine Mindestlänge von 15 Zeichen und den Verzicht auf Zeichenarten-Regeln kann Entra ID für Cloudkonten daher nicht technisch durchsetzen. Empfehlung von TOMORIS: Regeln Sie die Länge über Richtlinie, Einweisung und den Generator des Passwortmanagers und stützen Sie den Schutz auf MFA und Passkeys.

- ☐ Kennwortablauf prüfen: Mandanten, die vor 2021 angelegt wurden, haben standardmäßig 90 Tage. Microsoft empfiehlt für reine Cloudkonten, Kennwörter nie ablaufen zu lassen.
- ☐ MFA für alle Benutzer erzwingen: mit Conditional Access (Entra ID P1 oder P2) oder, ohne diese Lizenz, mit den Sicherheitsstandards (Security Defaults).
- ☐ Die globale Sperrliste ist immer aktiv; sie beruht laut Microsoft auf eigener Telemetrie zu Password-Spray-Angriffen. Ergänzen Sie unter Entra ID › Authentifizierungsmethoden › Kennwortschutz die benutzerdefinierte Liste: Firmen-, Produkt- und Ortsnamen, interne Begriffe; nur Grundbegriffe, Varianten erkennt der Algorithmus; höchstens 1.000 Begriffe; ab Entra ID P1.
- ☐ Bei lokalem Active Directory: Kennwortschutz mit dem Agenten auf den Domänencontrollern ausrollen, damit dieselben Sperrlisten auch dort gelten (Entra ID P1 oder P2).
- ☐ Smart Lockout prüfen: Standard ist eine Sperre nach 10 Fehlversuchen für 60 Sekunden mit steigender Dauer; anpassen am selben Ort (Entra ID P1). Bei Pass-Through-Authentifizierung: Entra-Schwelle kleiner, Entra-Sperrdauer länger als im lokalen AD.

- ☐ Passkeys (FIDO2) in der Richtlinie für Authentifizierungsmethoden aktivieren, in allen Editionen ohne Zusatzlizenz; für Admin-Rollen und sensible Ressourcen phishingresistente Anmeldung über die Authentifizierungsstärke in Conditional Access verlangen (Entra ID P1).
- ☐ Notfallkonten mit Passkey (FIDO2) oder zertifikatbasierter Authentifizierung ausstatten; Benutzerkonten, die Skripte ausführen, auf verwaltete Identitäten oder Dienstprinzipale umstellen.
- ☐ Identity-Protection-Risikoricthlinien aktivieren (Entra ID P2) und die Kennwortzurücksetzung mit einer Authenticator-App verbinden, wie Microsoft es für Microsoft 365 empfiehlt.

06

Vorgaben für Anmeldesysteme und eigene Anwendungen

Was Systeme prüfen, wie sie Fehlversuche begrenzen und wie sie Passwörter speichern, nach NIST und BSI.

- Sperrliste: Neue Passwörter vollständig gegen häufige, erwartbare und kompromittierte Passwörter prüfen, etwa Passwörter aus Datenlecks, Wörterbuchwörter, den Namen des Dienstes und den Benutzernamen; Ablehnung begründen und Hilfe zur Wahl anbieten (NIST 3.1.1.2).
- Länge: mindestens 15 Zeichen als einziger Faktor, mindestens 8 nur zusammen mit MFA; mindestens 64 Zeichen, alle druckbaren ASCII-Zeichen und Leerzeichen zulassen, Unicode nach Möglichkeit ebenso; das ganze Passwort prüfen, nie kürzen (NIST 3.1.1.2; ORP.4.A23).
- Fehlversuche: höchstens 100 in Folge je Konto, niedrigere Grenzen sind zulässig; ergänzend steigende Wartezeiten, etwa 30 Sekunden bis eine Stunde (NIST 3.2.2). Das BSI empfiehlt zunehmende Verzögerung und Sperre nach festgelegter Zahl (ORP.4.A13).
- Eingabe: Passwortmanager, automatisches Ausfüllen und Einfügen zulassen, das Passwort auf Wunsch anzeigen; keine Merkhilfen, keine Sicherheitsfragen (NIST 3.1.1.2). Bei Fehlanmeldung nicht verraten, ob Kennung oder Passwort falsch war (ORP.4.A23).
- Übertragung und Wechsel: Passwörter nur über verschlüsselte, authentifizierte Verbindungen; nach einem Wechsel keine alten Passwörter mehr zulassen (NIST 3.1.1.2; ORP.4.A23).
- Speicherung: gesalzen mit einem Passwort-Hashverfahren mit Kostenfaktor nach NIST SP 800-132, Salz mindestens 32 Bit, Kostenfaktor so hoch wie ohne Leistungseinbußen möglich und mit der Zeit erhöhen; empfohlen ist ein zusätzlicher Schritt mit geheimem Schlüssel, getrennt gespeichert, etwa in einem Hardware-Sicherheitsmodul (NIST 3.1.1.2; ORP.4.A12).

07 —

Häufige Fehler bei der Umstellung

Woran neue Passwortregeln in der Praxis scheitern und wie Sie es vermeiden.

- Den Zwangswechsel abschaffen, ohne Kompromittierungen erkennen zu können: Das BSI knüpft den Verzicht an Maßnahmen, die kompromittierte Passwörter erkennen (ORP.4.A23).
- Als NIS2-Einrichtung den Wechsel ganz abschaffen: Anhang Nr. 11.6.2 lit. c DVO 2024/2690 verlangt einen Wechsel in vorab festgelegten Zeitabständen. Wählen Sie den Abstand bewusst und begründet, statt ihn wegzulassen.
- Die Mindestlänge in der Richtlinie erhöhen, aber Systeme mit kurzer Höchstlänge behalten: Prüfen Sie, ob jedes System die volle Länge annimmt und prüft (ORP.4.A23; NIST 3.1.1.2).
- Einen Passwortmanager einführen, ohne die Synchronisierung über Onlinedienste Dritter zu bewerten: Wer nach IT-Grundschutz arbeitet, MUSS solche Funktionen deaktivieren (ORP.4.A8).
- MFA mit Einmalcode per App oder SMS für phishingresistent halten: Codes, die von Hand eingegeben werden, gelten nicht als phishingresistent; das leisten nur kryptografische Verfahren wie Passkeys (NIST 3.2.5).
- Notfallkonten von MFA ausnehmen: Microsoft wendet die Pflicht-MFA für Admin-Portale ausdrücklich auch auf Notfallkonten an.

08 —

Ausblick: Passkeys statt Passwörter

Warum Passkeys phishingresistent sind und was Microsoft Entra ID dafür heute schon bietet.

Passkeys beruhen auf FIDO2 und WebAuthn: Statt ein Passwort zu senden, weist das Gerät den Besitz eines privaten Schlüssels nach, freigegeben über eine PIN oder ein biometrisches Merkmal. NIST nennt WebAuthn als Beispiel für Phishingresistenz: Das Geheimnis ist an den authentifizierten Domainnamen des Dienstes gebunden, eine gefälschte Seite erhält deshalb nichts Verwertbares (SP 800-63B-4, 3.2.5).

- Passwörter sind nicht phishingresistent, ebenso wenig Verfahren mit manuell eingegebenem Code wie Einmalcodes oder Codes per SMS (NIST 3.1.1, 3.2.5).
- Synchronisierbare Passkeys, deren Schlüssel über einen Cloud-Dienst auf weitere Geräte kopiert werden, lässt NIST unter Auflagen zu, etwa dass der Schlüssel dort nur verschlüsselt liegt; für die höchste Stufe AAL3 sind sie ausgeschlossen (NIST 2.3.2, Anhang B).
- Entra ID unterstützt gerätegebundene Passkeys auf FIDO2-Sicherheitsschlüsseln und in Microsoft Authenticator sowie synchronisierte Passkeys; Letztere soll man laut Microsoft als phishingresistent, aber wie andere nicht attestierte Mittel behandeln. Gastkonten können keine Passkeys registrieren.

09 —

In vier Schritten zur neuen Richtlinie

Vom Bestand über Freigabe und Technik bis zur Einweisung und jährlichen Prüfung.

1

Bestand erheben

Systeme mit Passwortanmeldung, ihre heutigen Regeln sowie Administrator-, Dienst- und Notfallkonten auflisten.

2

Vorlage anpassen und freigeben

Platzhalter ausfüllen, Varianten entscheiden, Freigabe durch die Geschäftsführung einholen.

3

Technik umstellen

Ablauf, Sperrliste, Fehlversuchsgrenzen, MFA und Passkeys umsetzen, zuerst für Administratoren, Notfallkonten und Fernzugänge.

4

Einweisen und prüfen

Alle Mitarbeitenden einweisen (ORP.4.A19) und [jährlich] prüfen, ob Systeme die Regeln durchsetzen und sich Vorgaben geändert haben.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

10 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- NIST SP 800-63B-4: Digital Identity Guidelines, Authentication and Authenticator Management (endgültige Fassung, Juli 2025)**
Abstract, Notations, Abschnitte 2.2.2, 2.3.2, 3.1.1, 3.1.1.2, 3.2.2, 3.2.5, Anhang B; gelesen am 25.10.2026
doi.org/10.6028/NIST.SP.800-63B-4
- BSI IT-Grundschutz-Kompendium, Edition 2023: Baustein ORP.4 Identitäts- und Berechtigungsmanagement**
Kapitel 3 mit ORP.4.A1, A8 bis A14, A19, A21, A23 und A24; gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI: Sichere Passwörter erstellen**
Passwort-Check, Länge und Komplexität, Passwortmanager; gelesen am 25.10.2026
www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Info...
- NISG 2026, § 32 Risikomanagementmaßnahmen im Bereich der Cybersicherheit, tagesaktuelle Fassung im RIS**
§ 32 Abs. 1, 3, 4 lit. j und Abs. 5, gültig ab 1.10.2026; gelesen am 25.10.2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...

- 5 **NISV 2026, BGBl. II Nr. 290/2026, authentische Kundmachung im RIS**
§§ 2, 4 bis 7 und 9, kundgemacht am 1.10.2026, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 7 **Microsoft Learn: Empfehlungen zu Kennwortrichtlinien für Microsoft 365**
Einleitung, Kennwortrichtlinien für Administratoren und Benutzer; gelesen am 25.10.2026
learn.microsoft.com/microsoft-365/admin/misc/password-policy-re...
- 9 **Microsoft Learn: Kennwortrichtlinien und Kontoeinschränkungen in Microsoft Entra ID**
Kennwortrichtlinien von Microsoft Entra, Ablaufrichtlinien; gelesen am 25.10.2026
learn.microsoft.com/entra/identity/authentication/concept-sspr-...
- 11 **Microsoft Learn: Verpflichtende Multi-Faktor-Authentifizierung für Azure und Admin-Portale**
Durchsetzungsphasen 1 und 2, Konten, Vorbereitung, häufige Fragen; gelesen am 25.10.2026
learn.microsoft.com/entra/identity/authentication/concept-manda...
- 6 **Durchführungsverordnung (EU) 2024/2690, Anhang Nr. 11.6 und 11.7 (Authentifizierung)**
für alle wesentlichen und wichtigen Einrichtungen anwendbar nach § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 8 **Microsoft Learn: Beseitigen schwacher Kennwörter mit Microsoft Entra Kennwortschutz**
Globale und benutzerdefinierte Sperrliste, Bewertung, Hybridszenarien, Lizenzen; gelesen am 25.10.2026
learn.microsoft.com/entra/identity/authentication/concept-passw...
- 10 **Microsoft Learn: Schützen von Benutzerkonten mit Smart Lockout von Microsoft Entra**
Funktionsweise, Pass-Through-Authentifizierung, Verwalten der Sperrwerte; gelesen am 25.10.2026
learn.microsoft.com/entra/identity/authentication/howto-passwor...
- 12 **Microsoft Learn: Passkeys (FIDO2) in Microsoft Entra ID aktivieren**
Passkey-Profile, synchronisierte Passkeys, Authentifizierungsstärke, bekannte Probleme; gelesen am 25.10.2026
learn.microsoft.com/entra/identity/authentication/how-to-authen...