

TEMPLATE · TOMORIS TOOLBOX

Password Policy: Template Based on NIST and BSI

Policy text with placeholders, old and new rules with citations, and a checklist for Microsoft Entra ID, backed by NIST SP 800-63B-4, BSI ORP.4, and Microsoft Learn

UPDATED

Oct 25, 2026

LENGTH

PDF, 11 pages

ONLINE

tomoris.com/en/downloads/passwortrichtlinie-vorlage

AT A GLANCE

15

Characters minimum length without MFA (NIST SP 800-63B-4)

64

Characters maximum length to allow at a minimum (NIST)

No expiration

Change only on suspicion (NIST); NIS2: define an interval

MFA

Mandatory for Microsoft admin portals, named in the NISG

WHO IT IS FOR

- Executive management of small and medium-sized companies that want to issue a binding password policy
- IT management and information security officers who bring existing rules up to the NIST and BSI standard
- IT service providers that set up password rules and Microsoft Entra ID for their customers

WHAT THIS COVERS

Many password policies still require special characters and a change every 90 days. The current NIST SP 800-63B-4 of July 2025 prohibits both for authentication systems and relies on length, blocklists, and limited failed attempts; in IT-Grundschutz, the BSI advises against purely time-based changes. This template translates the requirements into policy text with placeholders, compares old and new rules with citations, and guides you through the implementation in Microsoft Entra ID.

This template must be adapted to your company, your systems, and your protection requirements and does not replace legal advice. The cited standards and vendor information in their current version are authoritative, and for entities under the NISG 2026, the statutory text in its current version. Microsoft features, names, and licenses may change.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01	What NIST and BSI require today	2
02	Old rule, new rule	3
03	Where multifactor authentication is mandatory	4
04	Template: password policy to adapt	5
05	Implementation in Microsoft Entra ID	7
06	Requirements for authentication systems and your own applications	8
07	Common mistakes during the transition	9
08	Outlook: passkeys instead of passwords	9
09	Four steps to the new policy	10
10	Sources	10

01 —

What NIST and BSI require today

The new basic rules at a glance and how binding the sources are for companies in Austria.

In July 2025, the US standards agency NIST published SP 800-63B-4 as the final version; it replaces the previous SP 800-63B. It is aimed at US government information systems and is not binding for companies in Austria, but it is suitable as a benchmark. SHALL means mandatory, SHOULD means recommended. For authentication systems, the following applies, among other things: at least 15 characters if the password is the only factor, no rules on character types, no change after a set period, a blocklist, and no more than 100 failed attempts (3.1.1.2, 3.2.2).

The IT-Grundschutz Compendium of the German BSI (Edition 2023) requires that password use be regulated in a binding manner (ORP.4.A8). Purely time-based changes SHOULD be avoided; instead, measures MUST

be taken to detect compromised passwords (ORP.4.A23). Basic requirements are to be met first; together with them, standard requirements constitute the state of the art. On its consumer page, the BSI recommends long passwords, such as five to six randomly chosen words with spaces, also mentions shorter passwords with four character types, and advises using a password manager.

Mandatory or recommended? NIST and IT-Grundschutz are standards, not laws in Austria. Multifactor authentication is named by law for essential and important entities in § 32 para. 4 lit. j NISG 2026 (Austrian Network and Information Systems Security Act 2026); the authentication requirements in the annex to Implementing Regulation (EU) 2024/2690 also apply to them (§ 2 NISV 2026, Austrian NIS Regulation 2026), see section 02. The template in this document is a TOMORIS recommendation based on these sources.

02

Old rule, new rule

Nine common password rules and what replaces them under NIST SP 800-63B-4 and BSI ORP.4.

Comparison with citations (NIST = SP 800-63B-4, ORP.4 = BSI IT-Grundschutz Edition 2023)

COMMON UNTIL NOW	NEW	CITATION
At least 8 characters with uppercase and lowercase letters, a digit, and a special character	Length instead of character types: at least 15 characters, at least 8 only in combination with MFA; no other composition rules	NIST 3.1.1.2; Microsoft recommends at least 14 characters for Microsoft 365
Change every 30, 60, or 90 days	No change after a set period; mandatory change on suspicion or evidence of compromise	NIST 3.1.1.2; ORP.4.A8, ORP.4.A23
Maximum length of 12 or 16 characters, spaces prohibited	Allow at least 64 characters, all printable characters, and spaces; check the full length	NIST 3.1.1.2; ORP.4.A23
No check against known passwords	Blocklist of common, expected, and compromised passwords; rejection with an explanation	NIST 3.1.1.2; ORP.4.A8
Pasting blocked, password managers discouraged	Allow password managers and autofill, permit pasting	NIST 3.1.1.2; ORP.4.A8 (review use)
Security question and password hint for resets	No security questions, no hints visible without signing in; secure reset procedure	NIST 3.1.1.2; ORP.4.A11
Unlimited sign-in attempts	Limit failed attempts: increasing delay and logout after a defined number, at most 100	NIST 3.2.2; ORP.4.A13
Password as the only protection, even for administrators	MFA, at least for administrators; offer a phishing-resistant method	ORP.4.A10, ORP.4.A21; NIST 2.2.2; § 32 para. 4 lit. j NISG 2026
Passwords stored in plain text or with reversible encryption	Stored salted and with a password hashing scheme	NIST 3.1.1.2; ORP.4.A12, ORP.4.A23

NIS2 entities: Under annex point 11.6.2 of Implementing Regulation (EU) 2024/2690, which § 2 NISV 2026 declares applicable, authentication credentials must be changed at the outset, at predefined intervals, and on suspicion (lit. c); after a defined number of unsuccessful sign-in attempts, a reset of the authentication credentials and a lockout must be required (lit. d); inactive sessions must be terminated (lit. e); and separate credentials must be used for privileged accounts (lit. f). You set the interval yourself and justify it with the risk analysis; the annex does not specify a minimum value.

03

Where multifactor authentication is mandatory

NISG 2026 for NIS2 entities and Microsoft for administrative access; the BSI recommends it (SHOULD) for administrators.

For essential and important entities, § 32 para. 4 lit. j NISG 2026 has, since October 1, 2026, included the "use of multifactor authentication or continuous authentication solutions" among the minimum contents of the risk management measures. They must be appropriate and proportionate (paras. 1 and 3). Details are set out in the NISV 2026 (BGBl. II No. 290/2026): its § 2 extends the annex of Implementing Regulation (EU) 2024/2690 to all essential and important entities not already covered by the regulation itself. Accordingly, users must be authenticated with multiple factors or continuously, where appropriate and depending on the classification of the assets (annex point 11.7.1).

Microsoft requires MFA for administrative access; opting out is not possible



Oct 2024

Admin portals

Azure portal, Microsoft Entra admin center, and Intune admin center: MFA for every administrative action, rolled out gradually in all tenants.



Feb 2025

Microsoft 365 admin center

Gradual enforcement of MFA when signing in to the Microsoft 365 admin center.



Oct 1, 2025

Tools and interfaces

Azure CLI, Azure PowerShell, Azure app, IaC tools, and REST API for create, update, and delete operations; a postponement was possible until July 1, 2026.

The Microsoft requirement applies to all user accounts, including emergency accounts; for these, Microsoft recommends a passkey (FIDO2) or certificate-based authentication. Managed identities and service principals are not affected, but user accounts that run scripts as service accounts are. In IT-Grundschutz, accounts with far-reaching privileges SHOULD be protected with multifactor authentication (ORP.4.A10), and generally so where protection requirements are high (ORP.4.A21). At level AAL2, NIST requires offering at least one phishing-resistant method (2.2.2).

TOMORIS recommendation: MFA for all accounts, at least for email, cloud services, remote access, and administration. This goes beyond the obligations named here.

04 —

Template: password policy to adapt

Model text with 15 clauses for all accounts, special accounts, and IT systems, plus the approval form to fill in.

How to adapt the template: replace all information in square brackets, choose one option where alternatives are separated by |, and delete what does not apply. Numbers such as [15] characters are TOMORIS suggestions based on the sources. Citations in parentheses show what a rule is based on; rules without a citation are organizational additions by TOMORIS.

1. Purpose and scope

This policy governs the selection, use, change, and verification of passwords at [Company]. It applies to all employees and external service providers with access to its systems and to all user, administrator, service, and emergency accounts. [Name, role] is responsible (ORP.4.A8).

2. Length instead of character rules

Passwords have at least [15] characters; systems allow at least [64] characters, all printable characters, and spaces. Requirements for character types are dropped where the system permits. Passphrases of five to six random words or passwords from the password manager are recommended. Avoid umlauts and ß because not every system accepts them (NIST 3.1.1.2; BSI).

3. Prohibited passwords

Passwords that are easy to guess, passwords from lists of common or leaked passwords, and passwords containing your own name, user name, or company, product, or location names are not permitted. Where possible, systems check new passwords against a blocklist and state the reason for rejection (ORP.4.A8; NIST 3.1.1.2).

4. One password per account

Each password applies to only one system or application and is never used for private or third-party services. Passwords are secret, known only to the person concerned, and are entered unobserved (ORP.4.A8; Microsoft recommendations for Microsoft 365).

5. Password manager

[Product] is approved as the password manager; its master password is particularly strong and used only there. Autofill and pasting are permitted. Outside of it, passwords are not written down, except for emergency deposit (clause 10). Synchronization via third-party online services: [disabled, mandatory under ORP.4.A8 | permitted after a documented risk assessment, deviation from ORP.4.A8] (ORP.4.A8; NIST 3.1.1.2; BSI).

6. Change only with cause

Passwords do not expire after set periods. A password is changed immediately if it has become known to unauthorized persons or if this is suspected; if there is evidence of compromise, IT enforces the change. Report any suspicion immediately to [Contact]. To detect compromised passwords, IT uses [Method]. [For NIS2 entities: In addition, passwords are changed every [interval].] (ORP.4.A8, ORP.4.A23; NIST 3.1.1.2; annex point 11.6.2(c) Implementing Regulation 2024/2690)

7. Multifactor authentication	A second factor is mandatory for [all accounts email, cloud services, remote access, and administration]. Permitted methods are [passkey (FIDO2), security key, authenticator app]; phishing-resistant methods such as passkeys are preferred (ORP.4.A10, ORP.4.A21; NIST 2.2.2; for NIS2 entities § 32 para. 4 lit. j NISG 2026).
8. Reset without security questions	There are no security questions and no hints that are visible without signing in. Forgotten passwords are reset via [self-service with a second factor identity verification by the help desk]; those authorized to reset passwords are trained for this (NIST 3.1.1.2; ORP.4.A11).
9. Administrator accounts	Accounts with far-reaching privileges are assigned to one person and always protected with MFA, preferably with a passkey (FIDO2), security key, or certificate; shared administrator accounts are not permitted. [Where protection requirements are high: four-eyes principle.] (ORP.4.A1, A10, A14, A24)
10. Emergency accounts	The [number] emergency accounts are protected with [passkey (FIDO2) certificate]; their credentials are kept [sealed, location], and written deposit is permitted only for this purpose. [Name, role] and [Name, role] have access. Every use is documented, after which the credentials are changed (ORP.4.A8; Microsoft mandatory MFA).
11. Service and technical accounts	Service accounts receive randomly generated passwords with at least [length] characters, managed in [Product]. Automation in Azure uses managed identities or service principals instead of user accounts. Password changes are coordinated with [application owners] (ORP.4.A23; NIST 3.1.1.2; Microsoft).
12. Default passwords	Preset passwords and predefined accounts are changed before productive use, and default passwords are replaced with passwords that comply with this policy (ORP.4.A9, ORP.4.A23).
13. Requirements for IT systems	Systems check the complete password, lock for at least [60] seconds after [10] failed attempts with increasing duration, do not reveal whether the account name or the password was wrong, do not allow old passwords to be reused, terminate inactive sessions after [minutes], [for NIS2 entities: lock the account after [number] failed attempts and require a new password,] transmit only in encrypted form, and store passwords salted with a password hashing scheme (NIST 3.1.1.2, 3.2.2; ORP.4.A13, A23; annex point 11.6.2(d) and (e) Implementing Regulation 2024/2690).
14. Instruction, exceptions, monitoring	All employees are instructed when they join and [annually] (ORP.4.A19). [Name, role] approves exceptions in writing, with reasons, and for a limited time; [Name, role] reviews the implementation [annually].
15. Entry into force	This policy applies from [MM/DD/YYYY], replaces [previous rules], and is reviewed [annually] and whenever the underlying standards change.

Approval and key data to fill in

ITEM	ENTRY
Company	_____
Responsible for the policy (name, role)	_____
Password manager and permitted MFA methods	_____
Reporting contact in case of suspicion	_____
Valid from, next review	_____
Approval by executive management (name, date, signature)	_____

05 —

Implementation in Microsoft Entra ID

What is fixed, what you can configure, and which license you need for it.

For accounts created and managed directly in Entra ID, a fixed password policy applies: 8 to 256 characters, three of four character types (lowercase and uppercase letters, digits, symbols), no Unicode characters. Only the expiration can be changed. For accounts synchronized from on-premises Active Directory, it applies only if the cloud password policy for synchronized users is explicitly enabled.

Entra ID therefore cannot technically enforce a minimum length of 15 characters and the elimination of character type rules for cloud accounts. TOMORIS recommendation: govern length through the policy, instruction, and the password manager's generator, and base protection on MFA and passkeys.

- ☐ Check password expiration: tenants created before 2021 have 90 days by default. For cloud-only accounts, Microsoft recommends never letting passwords expire.
- ☐ Enforce MFA for all users: with Conditional Access (Entra ID P1 or P2) or, without this license, with security defaults.
- ☐ The global banned password list is always active; according to Microsoft, it is based on its own telemetry on password spray attacks. Add the custom list under Entra ID › Authentication methods › Password protection: company, product, and location names, internal terms; only base terms, the algorithm detects variants; at most 1,000 terms; Entra ID P1 or higher.
- ☐ With on-premises Active Directory: roll out password protection with the agent on the domain controllers so that the same banned lists apply there too (Entra ID P1 or P2).
- ☐ Check smart lockout: the default is a lockout after 10 failed attempts for 60 seconds with increasing duration; adjust it in the same place (Entra ID P1). With pass-through authentication: Entra threshold lower, Entra lockout duration longer than in on-premises AD.

- ☐ Enable passkeys (FIDO2) in the authentication methods policy, in all editions without an additional license; for admin roles and sensitive resources, require phishing-resistant sign-in via authentication strength in Conditional Access (Entra ID P1).
- ☐ Equip emergency accounts with a passkey (FIDO2) or certificate-based authentication; switch user accounts that run scripts to managed identities or service principals.
- ☐ Enable Identity Protection risk policies (Entra ID P2) and combine password reset with an authenticator app, as Microsoft recommends for Microsoft 365.

06 —

Requirements for authentication systems and your own applications

What systems check, how they limit failed attempts, and how they store passwords, according to NIST and BSI.

- Blocklist: check new passwords in full against common, expected, and compromised passwords, such as passwords from data breaches, dictionary words, the name of the service, and the user name; explain the rejection and offer help with choosing (NIST 3.1.1.2).
- Length: at least 15 characters as the only factor, at least 8 only in combination with MFA; allow at least 64 characters, all printable ASCII characters, and spaces, and Unicode where possible; check the entire password, never truncate it (NIST 3.1.1.2; ORP.4.A23).
- Failed attempts: at most 100 consecutive attempts per account, lower limits are permitted; in addition, increasing wait times, for example 30 seconds to one hour (NIST 3.2.2). The BSI recommends increasing delays and a lockout after a defined number (ORP.4.A13).
- Input: allow password managers, autofill, and pasting, show the password on request; no hints, no security questions (NIST 3.1.1.2). On a failed sign-in, do not reveal whether the account name or the password was wrong (ORP.4.A23).
- Transmission and change: passwords only over encrypted, authenticated connections; after a change, no longer allow old passwords (NIST 3.1.1.2; ORP.4.A23).
- Storage: salted with a password hashing scheme with a cost factor according to NIST SP 800-132, salt at least 32 bits, cost factor as high as possible without performance loss and increased over time; an additional step with a secret key, stored separately, for example in a hardware security module, is recommended (NIST 3.1.1.2; ORP.4.A12).

07 —

Common mistakes during the transition

Where new password rules fail in practice and how to avoid it.

- Abolishing forced changes without being able to detect compromises: the BSI makes dropping them conditional on measures that detect compromised passwords (ORP.4.A23).
- Abolishing changes entirely as a NIS2 entity: annex point 11.6.2(c) Implementing Regulation 2024/2690 requires a change at predefined intervals. Choose the interval deliberately and with reasons instead of omitting it.
- Raising the minimum length in the policy but keeping systems with a short maximum length: check whether every system accepts and checks the full length (ORP.4.A23; NIST 3.1.1.2).
- Introducing a password manager without assessing synchronization via third-party online services: anyone working according to IT-Grundschutz MUST disable such functions (ORP.4.A8).
- Considering MFA with a one-time code via app or SMS to be phishing-proof: codes entered by hand are not considered phishing-resistant; only cryptographic methods such as passkeys achieve this (NIST 3.2.5).
- Exempting emergency accounts from MFA: Microsoft explicitly applies mandatory MFA for admin portals to emergency accounts as well.

08 —

Outlook: passkeys instead of passwords

Why passkeys are phishing-resistant and what Microsoft Entra ID already offers for them today.

Passkeys are based on FIDO2 and WebAuthn: instead of sending a password, the device proves possession of a private key, unlocked with a PIN or a biometric feature. NIST cites WebAuthn as an example of phishing resistance: the secret is bound to the authenticated domain name of the service, so a fake site receives nothing usable (SP 800-63B-4, 3.2.5).

- Passwords are not phishing-resistant, nor are methods with a manually entered code such as one-time codes or codes via SMS (NIST 3.1.1, 3.2.5).
- NIST permits syncable passkeys, whose keys are copied to other devices via a cloud service, subject to conditions, for example that the key is stored there only in encrypted form; they are excluded for the highest level, AAL3 (NIST 2.3.2, Appendix B).
- Entra ID supports device-bound passkeys on FIDO2 security keys and in Microsoft Authenticator as well as synced passkeys; according to Microsoft, the latter should be treated as phishing-resistant but like other non-attested methods. Guest accounts cannot register passkeys.

09 —

Four steps to the new policy

From taking stock through approval and technology to instruction and annual review.

1

Take stock

List systems with password sign-in, their current rules, and administrator, service, and emergency accounts.

2

Adapt and approve the template

Fill in placeholders, decide on alternatives, obtain approval from executive management.

3

Switch the technology

Implement expiration, blocklist, failed attempt limits, MFA, and passkeys, first for administrators, emergency accounts, and remote access.

4

Instruct and review

Instruct all employees (ORP.4.A19) and check [annually] whether systems enforce the rules and whether requirements have changed.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)

tomoris.com/tools/nis2-check

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 **NIST SP 800-63B-4: Digital Identity Guidelines, Authentication and Authenticator Management (final version, July 2025)**
Abstract, Notations, sections 2.2.2, 2.3.2, 3.1.1, 3.1.1.2, 3.2.2, 3.2.5, Appendix B; accessed October 25, 2026
doi.org/10.6028/NIST.SP.800-63B-4
- 2 **BSI IT-Grundschutz Compendium, Edition 2023: module ORP.4 Identity and Access Management**
Chapter 3 with ORP.4.A1, A8 to A14, A19, A21, A23, and A24; accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **BSI: Creating secure passwords**
Password check, length and complexity, password managers; accessed October 25, 2026
www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Info...
- 4 **NISG 2026, § 32 Cybersecurity risk management measures, current daily version in the RIS**
§ 32 paras. 1 and 3, para. 4 lit. j, and para. 5, valid from October 1, 2026; accessed October 25, 2026
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...

- 5 NISV 2026, BGBl. II No. 290/2026, authentic promulgation in the RIS**
§§ 2, 4 to 7, and 9, promulgated on October 1, 2026, accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 7 Microsoft Learn: Password policy recommendations for Microsoft 365**
Introduction, password policies for administrators and users; accessed October 25, 2026
learn.microsoft.com/microsoft-365/admin/misc/password-policy-re...
- 9 Microsoft Learn: Password policies and account restrictions in Microsoft Entra ID**
Microsoft Entra password policies, expiration policies; accessed October 25, 2026
learn.microsoft.com/entra/identity/authentication/concept-sspr-...
- 11 Microsoft Learn: Mandatory multifactor authentication for Azure and admin portals**
Enforcement phases 1 and 2, accounts, preparation, frequently asked questions; accessed October 25, 2026
learn.microsoft.com/entra/identity/authentication/concept-manda...
- 6 Implementing Regulation (EU) 2024/2690, annex points 11.6 and 11.7 (authentication)**
Applicable to all essential and important entities under § 2 NISV 2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 8 Microsoft Learn: Eliminate bad passwords using Microsoft Entra Password Protection**
Global and custom banned password lists, evaluation, hybrid scenarios, licenses; accessed October 25, 2026
learn.microsoft.com/entra/identity/authentication/concept-passw...
- 10 Microsoft Learn: Protect user accounts from attacks with Microsoft Entra smart lockout**
How it works, pass-through authentication, managing lockout values; accessed October 25, 2026
learn.microsoft.com/entra/identity/authentication/howto-passwor...
- 12 Microsoft Learn: Enable passkeys (FIDO2) in Microsoft Entra ID**
Passkey profiles, synced passkeys, authentication strength, known issues; accessed October 25, 2026
learn.microsoft.com/entra/identity/authentication/how-to-authen...