B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

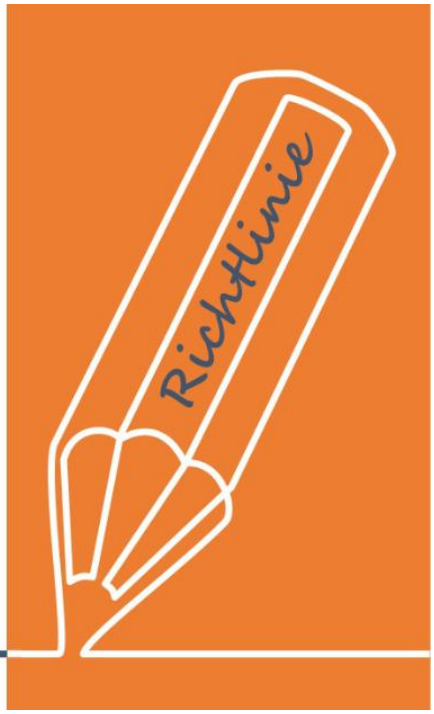
Richtlinie zur Nutzung von Kennwörtern

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Richtlinie zur Nutzung von Kennwörtern

des Unternehmens



Inhaltsverzeichnis

1. Zweck und Zielsetzung

Diese Passwortrichtlinie regelt die Gestaltung und die Handhabung der Passwörter, die zur Authentisierung von berechtigten Benutzern verwendet werden. Sie ist im Rahmen der technischen Möglichkeiten auf alle EDV-Systeme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und damit verbundener missbräuchlicher Verwendung oder Veränderung geschützt werden müssen.

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten, Dienstleister und alle anderen relevanten Personen, die auf die unternehmensrelevanten Bereiche dieser IT-Systeme und geschützten Informationen des Unternehmens zugreifen.

3. Verhaltensregeln beim Umgang mit Passwörtern

Die Einhaltung der Passwortrichtlinie wird durch die jeweiligen Vorgesetzten kontrolliert und ist durch Maßnahmen im Rahmen der Dienstaufsicht sicherzustellen. Die Beschäftigten sind mindestens einmal jährlich, oder bei wesentlichen Änderungen der Passwortvorgaben, über den Inhalt dieser Richtlinie zu informieren. Die nachfolgenden Informationen geben eine Erläuterung, wie die Zielsetzungen dieser Richtlinie in die operative Büroorganisation umzusetzen sind.

3.1 Initiale Wahl von Passwörtern

- Benutzerkennungen sollen personenbezogen vergeben werden (nicht „rollenbezogen“ für mehrere Personen).
- Für jeden Dienst ist ein eigenes Passwort zu verwenden. Ausgenommen sind Single Sign-on Dienste.
- Werden Passwörter bei der Installation von Software automatisch vergeben, sind diese beim darauffolgenden Erstzugriff zu ersetzen.
- Passwörter sollten möglichst zufällig erzeugt werden. Die Verwendung eines Passwortgenerators in Verbindung mit einem Passwortmanager (siehe Aufbewahrung von Passwörtern) wird empfohlen.
- Alternativ können Passwort-Sätze (Passphrase) verwendet werden, um gut merkbare Passwörter zu erhalten.
- Für die Sicherheit sonstiger anwendungsbezogener Passwörter, die nicht im Zusammenhang mit dem Anmelden (Login) einzugeben sind, gelten die gleichen Vorgaben wie für die Passwörter. Für Anwendungen oder Sicherheitsgründe kann von den Vorgaben abgewichen werden.
- Die Aufhebung einer Passwortsperre ist nur dann möglich, wenn die Identität des Benutzers eindeutig festgestellt wurde. Das Aufheben einer Sperrung und die Passwortneutralisierung sind veränderungssicher zu dokumentieren.

3.2 Nutzung von Passwörtern

- Bei der Eingabe von Passwörtern ist darauf zu achten, dass die Eingabe nicht beobachtet wird. Sie dürfen während der Eingabe nicht in Klartext angezeigt werden.
- Passwörter müssen geheim gehalten werden und dürfen nur dem Benutzer persönlich bekannt sein.
- Passwörter dürfen nicht weitergegeben werden.
- Ist ein Passwort unautorisierten Personen bekannt geworden oder besteht der Verdacht dazu, ist das Passwort zu ändern.
- Passwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses verwendet werden, z.B. in einer Funktionstaste oder im Passwortspeicher eines Internet-Browsers.
- System-Administratorpasswörter dürfen nur den Personen bekannt sein, die sie zur Erledigung der ihnen übertragenen Aufgaben benötigen. Verlässt eine Person den Kreis der Berechtigten, sind die betroffenen Passwörter umgehend zu ändern.

3.3 Aufbewahrung von Passwörtern

- Es ist nicht zulässig Passwörter auf IT-Systemen unverschlüsselt zu speichern.
- Die Passwortdateien der Benutzer sind vor unbefugtem Zugriff zu schützen. Eine verschlüsselte Speicherung in einem sicheren Passwortmanager wird empfohlen. Ein geeignetes Tool wird durch das Unternehmen bereitgestellt.
- Passwörter dürfen nicht im Klartext notiert und für Dritte einsehbar sein, beispielsweise als Post-It am Bildschirm oder als Notiz unter der Tastatur.
- Bei der physischen Hinterlegung muss das Passwort in einem versiegelten Umschlag sicher aufbewahrt werden (z.B. Tresor).

3.4 Zwei-Faktor-Authentifizierung (2FA)

Eine sicherere Art, Zugänge zu Systemen abzusichern, ist die Zwei-Faktor-Authentifizierung. Diese Art der Authentifizierung ist für alle Zugänge aus dem Internet auf IT-Systeme vorgeschrieben, soweit das technisch möglich ist. Bei kritischen Systemen, auf denen streng vertrauliche Informationen verarbeitet oder gespeichert werden, ist diese Art der Authentifizierung in die Sicherheitsarchitektur einzubeziehen und als Authentifizierung in Erwägung zu ziehen, sofern dies technisch möglich, wirtschaftlich und praktikabel ist.

Werden zusätzliche Authentifizierungsmittel eingesetzt (z.B. Magnetkarten, Chipkarten, Authenticator), müssen sie so gehandhabt werden, dass sie vor dem Missbrauch durch Dritte geschützt sind. Sofern erforderlich, sind die zuständigen Stellen hierzu besondere Regelungen.

3.5 Anonyme Benutzerkennungen

Anonyme Benutzerkennungen sind regulär zu vermeiden. Benutzerkennungen müssen personenbezogen vergeben werden, d.h. einem Benutzer zuordenbar sein. Ausnahmen bilden Systemkennungen und Spezialkennungen für technische Abläufe.

4. Anforderungen an Passwörter

Die nachfolgenden Anforderungen stellen Mindestanforderungen für Kennwörter vorgegeben. Für spezielle Anwendungen, die den Zugang zu vertraulichen oder sehr vertraulichen Informationen ermöglichen, sollten die Anforderungen an Passwörter ggf. erhöht werden.

- Ein Passwort muss mindestens 12 Zeichen lang sein.
- Ein Passwort muss jeweils mindestens 2 Zeichen aus folgenden Zeichenarten enthalten:
  - Großbuchstaben: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z
  - Kleinbuchstaben: a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z
  - Ziffern: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
  - Sonderzeichen: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ]
- Ein Passwort darf kein mehr als 4-mal hintereinander wiederholtes Zeichen enthalten.
- Es sollten im Passwort keine persönlichen Daten, Namen oder die Rollen der Anwender enthalten sein.
- Es dürfen keine bekannten Wörter aus einem Wörterbuch verwendet werden

Im Falle von administrativen Accounts gelten die folgenden zusätzlichen Anforderungen an Passwörter:

- Ein Passwort muss mindestens 20 Zeichen lang sein.
- Das Passwort wurde unter Berücksichtigung der vorher genannten Vorgaben mit einem Passwortgenerator erzeugt.

5. Sonstige technisch-organisatorische Maßnahmen

Das Unternehmen behält sich vor, direkt beim Setzen eines Passwortes technische Maßnahmen zum Überprüfen der geltenden Richtlinie einzusetzen. Daneben sind folgende technisch-organisatorische Maßnahmen zu berücksichtigen.

- Nach der vorgegebenen Frist (z.B. 180 Tage) wird ein Passwortwechsel erzwungen. Für den regelmäßigen Wechsel von Passwörtern wird bevorzugt ein automatisiertes Verfahren eingesetzt.
- Neu eingesetzte Benutzerkennungen, die länger als 90 Tage nicht aktiviert wurden, werden überprüft und bei Bedarf gesperrt.
- Passwörter dürfen in Netzwerken nur verschlüsselt übertragen werden.
- Bei öffentlich zugänglichen Einrichtungen sind geeignete Maßnahmen zur Abwehr von Brute-Force-Angriffen zum Erraten von Passwörtern zu treffen. (z.B. 10 Versuche bis zum Sperren der Kennung des Benutzers (manuelles Entsperren durch einen Administrator notwendig)
- Bei der Auswahl von IT-Systemen und Anwendungsprogrammen sind die vorher genannten Mechanismen im Lastenheft als „Muss-Funktion“ aufzuführen. Sofern dies (z.B. aus betriebswirtschaftlichen Gründen) nicht möglich ist, muss eine geeignete Zusatz-Software eingesetzt werden.

6. Einhaltung bzw. Nichtbeachtung der Richtlinie

Damit diese Regelung [illegible] Hilfe aller. Die Einhaltung dieser Regelung wird von den Führungskräften stichprobenartig kontrolliert. **Nichteinhaltung dieser Richtlinie kann zu disziplinarischen Maßnahmen führen, einschließlich Abmahnung, Kündigung oder rechtlichen Schritten.**

7. Dokumentenlenkung und Änderungshistorie

Diese Richtlinie wird über das Intranet zur Verfügung gestellt.

Dokumentenlenkung

Lenkungskriterien	
Klassifizierung der Wichtigkeit (1-10)	
Klassifizierung der Vertraulichkeit	☐ Öffentlich ☐ Intern ☐ Vertraulich ☐ Streng vertraulich
Speicherort	[z.B. URL der Datei auf dem Server]
Verantwortlicher	
Aktuelle Version	1.0
Datum Erstellung / letzte Änderung	19.11.2025
Nächstes Dokumenten-Review	19.11.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	5		

Hinweise zur Nutzung der Vorlage

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine „Richtlinie Clean Desk“ darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit oder Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.

Jede Person, die dieses Produkt erwirbt ist verpflichtet, ihre individuellen Ergänzungen und Anpassungen vorzunehmen und alle Inhalte für den eigenen Anwendungsfall zu prüfen, d.h. diese ggf. mit eigenen Texten zu erweitern oder nicht passende Inhalte zu entfernen.

Die nachfolgende Liste gibt Ihnen einige Hinweise, worauf Sie bei der Ergänzung mit eigenen Texten bzw. Textmodulen unbedingt achten sollten:

1. Wählen Sie einfache, allgemein verständliche Formulierungen und schreiben Sie keine „Bandwurmsätze“.
2. Benutzen Sie eine verständliche Wortwahl und erklären Sie nicht vermeidbares Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.
5. Schreiben Sie gendergerecht. Die Nennung aller Geschlechter drückt die Wertschätzung gegenüber allen Menschen aus, unabhängig ihres Geschlechts.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

(1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
(2) Für Garantien haftet der Lizenzgeber unbeschränkt.
(3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
(4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
(5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
(6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
(7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
(8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.