Passwortrichtlinie (BASIC)

 Vorlage

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung**  |  |
| Autor  |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von  |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Datum der Genehmigung** | **Genehmigt durch**  | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# Intro

Passwörter werden häufig zur Authentifizierung von Benutzern verwendet. Dieses Dokument enthält eine Richtlinie für die Verwendung und Umsetzung von Passwörtern für vertrauliche und kritische Informationssysteme.

Früher dachten wir, dass die beste Art Passwörter zu schützen, darin bestand sie stark zu machen und sie oft zu ändern. Heutzutage gewinnt die neue Philosophie, nämlich Passwörter lang, aber benutzerfreundlich zu gestalten, immer mehr an Popularität. Die Multi-Faktor-Authentifizierung wird nachdrücklich empfohlen und sollte wann immer möglich verwendet werden, nicht nur für arbeitsbezogene Konten, sondern auch für persönliche Konten.

Dieses Grundsatzdokument ist Teil einer Reihe von Grundsatzdokumenten, die **[Organisation]** bei der Entwicklung einer soliden Strategie für die Cybersicherheit unterstützen.

# Passwort-Einstellungen

## Passwortstärke

Die Stärke des Passworts ist wichtig, um die Gefahr des Missbrauchs zu verringern.

Passwortsysteme sollten die Verwendung von sicheren Passwörtern nach diesen Regeln erzwingen:

* Die Mindestlänge des Passworts muss eingehalten werden **(mindestens X Zeichen, X wird empfohlen).**
* Administrator-Passwörter müssen mindestens **XX** Zeichen enthalten.
* Passwörter für Dienstkonten müssen mindestens **XX** Zeichen lang sein.
* Sehr lange Passwörter sollten erlaubt sein (z. B. 256 Zeichen).
* Passwörter, die Ihren Benutzernamen enthalten, sollten abgelehnt werden.
* Passwörter, die Ihren Vor- oder Nachnamen enthalten, sollten abgelehnt werden.
* Es müssen komplexe Passwörter erzwungen werden, die mindestens drei der folgenden Kategorien enthalten:
	+ Großbuchstaben (A-Z).
	+ Kleinbuchstaben (a-z).
	+ Ziffern (0-9).
	+ Sonderzeichen: !@#$%^&\*() usw.

Ausnahmen:

In den folgenden Fällen ist ein Passwort mit mindestens 4 Ziffern zulässig:

* Wenn der Code ein Zusatz zu einer physischen Zugangskennung wie einer Chipkarte oder einem Token ist.
* Wenn das System nicht an ein Netzwerk angeschlossen ist und über starke physische Sicherheitskontrollen verfügt.
* Wenn es zum entsperren des Bildschirms eines mobilen Geräts der **[Organisation]**, z.B. eines Smartphones oder Tablets verwendet wird.

## Richtlinie zur Änderung von Passwörtern

Um das Risiko der Kompromittierung von Passwörtern zu verringern, sollten sie regelmäßig geändert werden. Es gelten die folgenden Regeln:

* Die Standardkennwörter für neue Geräte sollten geändert werden.
* Die Systeme sollten es den Benutzern ermöglichen, ihre Passwörter jederzeit zu ändern.
* Regelmäßige Änderungen des Kennworts sollten in Abhängigkeit von der vom System vorgegebenen Mindestlänge des Kennworts erzwungen werden.
* Wenn die minimal zulässige Kennwortlänge des Systems **X** Zeichen beträgt, sollten die Benutzer gezwungen werden, ihre Kennwörter alle **X** Monate (oder **XX** Tage) zu ändern.
* Wenn die minimal zulässige Kennwortlänge des Systems **XX** Zeichen beträgt, sollten die Benutzer gezwungen werden, ihre Kennwörter alle **X** Monate (oder **XX** Tage) zu ändern.
* Passwörter, die von anderen als dem Nutzer selbst vergeben werden (z. B. von der IKT-Abteilung), sollten bei der ersten Anmeldung geändert werden.
* Passwortsysteme sollten die Wiederverwendung zumindest der letzten **X** Passwörter ausdrücklich verbieten.
* Gemeinsame Passwörter, die Personen bekannt sind, die die Organisation verlassen, sollten geändert werden.

Ausnahmen:

Das Ändern von Passwörtern wird in den folgenden Fällen empfohlen, ist aber nicht zwingend erforderlich:

* Wenn das Kennwort für ein Dienstkonto verwendet wird und nicht für die interaktive Anmeldung genutzt werden kann.
* Wenn der Code ein Zusatz zu einer physischen Zugangskennung wie einer Chipkarte oder einem Token ist.
* Wenn das System nicht an ein Netzwerk angeschlossen ist und über starke physische Sicherheitskontrollen verfügt.
* Wess es zum entsperren des Bildschirms eines mobilen Geräts der **[Organisation]**, z.B. eines Smartphones oder Tablets verwendet wird.

## Prävention von Angriffen

Systeme sollten über mindestens einen Mechanismus zur Verhinderung von Brute-Force-Angriffen verfügen. Beispiele für solche Techniken sind:

* **Kontosperrung:**
Eine Ausschlussrichtlinie deaktiviert die Anmeldefunktionalität für ein bestimmtes Konto. (z.B. Konto für **XX** Minuten sperren nach **X** fehlgeschlagenen Anmeldeversuchen).
* **Schwarze IP-Liste**:

Wie bei der Kontosperrung werden auch hier fehlgeschlagene Anmeldeversuche erkannt, aber es wird geprüft, von welchen IP-Adressen die Anmeldeanforderung stammt. Werden zu viele Versuche (z. B. 20) von einer bestimmten IP-Adresse festgestellt, wird diese Adresse auf eine schwarze Liste gesetzt.

* **Anmeldeverzögerung:**Dieser Mechanismus fügt eine stufenweise Wiederholungsverzögerung hinzu, nachdem ein falsches Passwort verwendet wurde. (z. B. 0,5 Sekunden nach zwei Fehlversuchen, 1 Sekunde nach dem dritten Fehlversuch, 2 Sekunden nach dem vierten, 4 Sekunden nach dem fünften, usw.).

# Passwortschutz

* Passwörter sollten nicht an Dritte weitergegeben werden, auch nicht an Vorgesetzte und Kollegen. Alle Passwörter sollten als sensible, vertrauliche Informationen der **[Organisation**] behandelt werden.
* Passwörter sollten nicht in E-Mail-Nachrichten oder anderen Formen der elektronischen Kommunikation enthalten sein und auch nicht telefonisch mitgeteilt werden.
* Passwörter sollten nur in von der Organisation zugelassenen Passwortmanagern gespeichert werden. Passwörter in Papierform sollten vermieden werden, es sei denn, es besteht ein starker physischer Schutz (z.B. ein Safe).
* Verwenden Sie nicht die Funktion "Passwort speichern" von Anwendungen (z. B. Webbrowsern).
* Jeder, der den Verdacht hat, dass sein Passwort missbraucht wurde, sollte dies melden und alle relevanten Passwörter ändern.

## Verteilung per E-Mail

Die Weitergabe von Benutzernamen und Kennwörtern per E-Mail kann effizient und bequem sein. Obwohl E-Mail standardmäßig nicht das sicherste Medium ist, kann es verwendet werden, wenn:

* Es wird kein externes E-Mail-System verwendet.
* E-Mails werden verschlüsselt gesendet (wie bei Office 365).
* Die angegebene Kombination aus Benutzername und Passwort verfällt nach der ersten Verwendung oder, wenn sie nicht verwendet wird, nach **1 Monat.**

## Verteilung per SMS

SMS ist kein sicheres Protokoll und sollte niemals zum Versenden von Kombinationen aus Benutzernamen und Passwort verwendet werden. Es kann verwendet werden, um teilweise Anmeldeinformationen zu senden, aber nur, wenn die folgenden Bedingungen erfüllt sind:

* Die Nachricht enthält höchstens einen Teil der Kombination: System, Benutzername, Passwort oder Token. Die anderen Teile werden über andere Verteilungsmethoden gesendet.
* Der Nutzer erwartet die Nachricht und wird sie daher wahrscheinlich bald nutzen.
* Die Informationen in der Nachricht verfallen nach der ersten Nutzung oder, wenn sie nicht genutzt werden, nach 1 Monat.