

# managedhosting.de

## Passwortrichtlinie

managedhosting.de GmbH
Friedrichstr. 191

10117 Berlin

Berlin, den 01.01.2016

# Passwortrichtlinie

## Inhaltsverzeichnis

# Präambel

Passwörter stellen in Kombination mit zusätzlichen Verfahren den wichtigsten Baustein der Zugangskontrolle dar. Sichere Passwörter und deren aufgabengerechte Zuteilung und Verwaltung ist ein wesentlicher Bestandteil bei der Umsetzung unserer IT- Sicherheitsrichtlinien.

# Geltungsbereich

(1) Diese Richtlinie regelt die Gestaltung und Handhabung von Passwörtern, die zur Authentifizierung berechtigter Benutzer eingesetzt werden.

(2) Sie ist im Rahmen der technischen Möglichkeiten auf alle IuK-Systeme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen. Auf Telekommunikationseinrichtungen ist sie anzuwenden, soweit dem nicht technische Einschränkungen entgegenstehen.

# Regeln im Umgang mit Passwörtern

(1) Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht unverschlüsselt gespeichert oder auf Funktionstasten hinterlegt werden.

(2) Die Länge der Passwörter richtet sich nach dem Schutzbedarf der Daten und Ressourcen. Sie beträgt mindestens 8 Stellen. Benutzerkennungen mit besonderen Rechten und Aufgaben (z.B. Systemverwaltung, Sicherheitsfunktionen oder Anwendungen mit sensiblen Daten) sind mit Passwörtern zu schützen, die mehr als 8 Zeichen umfassen

(3) Passwörter sollen technisch so komplex wie möglich zusammengesetzt sein (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). Dies ist der wesentlichste Schutz vor systematischem Ausspähen.

(4) Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:

- Zeichenwiederholungen,
- Zahlen und Daten aus dem Lebensbereich des Benutzers,
- Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen,
- einfache Ziffern- und Buchstabenkombinationen,
- Zeichen, die durch nebeneinander liegende Tasten eingegeben werden,
- Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter).

(5) Passwörter sind nach einer dem Schutzbedarf der Daten und Ressourcen angemessenen Frist zu ändern.

(6) Passwörter dürfen in der Regel höchstens einmal am Tag geändert werden. Sie sind jedoch unverzüglich zu ändern, wenn der Verdacht besteht, dass sie Dritten bekannt geworden sein könnten.

(7) Einstiegs- und Übergangspasswörter sind unverzüglich durch eigene Passwörter zu ersetzen.

(8) Endgeräte sind mit passwortgeschützten Bildschirmschonern bzw. Bildschirmabschaltungen zu versehen, die je nach Schutzwürdigkeit der Daten und Ressourcen nach einer bestimmten Zeit den Zugriff auf das angemeldete Endgerät verhindern. Für die Entsperrung mittels Passwort gelten die Regeln dieser Richtlinied.

(9) Sämtlicher Mitarbeiter, insbesondere die der IT- Administration haben die Grundregeln beim Umgang mit Passwörtern zu beachten. Untersagt ist insbesondere

- die Weitergabe eines Passworts an einen Kollegen, zum Beispiel bei Urlaubsvertretung
- die Verwendung des immer gleichen Passworts über viele Monate und Jahre hinweg
- die Auswahl zu kurzer, zu einfacher, in Wörterbüchern zu findender Passwörter
- das Notieren von Passwörtern
- die Nutzung immer des gleichen Passworts für alle internen und externen Anwendungen
- die ungeschützte Hinterlegung von Notfallpasswörtern
- die Unterlassung des Vier-Augen-Prinzips für besonders sensible Bereiche
- die unverschlüsselte Speicherung von Passwörtern

# Pflichten der IT- Administration

(1) Passwortdateien sind vor unbefugtem Zugriff zu schützen. Zur Speicherung von Passwörtern ist ein für den jeweiligen Einsatzzweck geeignetes und praktikables Verfahren zu wählen. Die Speicherung von Passwörtern auf Arbeitsgeräten der IT- Administration erfolgt mittels KeePass[1]. Die zentrale Verwaltung von Passwörtern erfolgt mittels Team Password Manager[2]. Die Speicherung von Passwortdateien für DR- Zwecke erfolgt auf einem - ausschließlich einem namentlich benannten Personenkreis zugänglichen - Datenspeicher in einer Passwortgeschützten .ZIP-Datei. Hierfür ist ein geeignetes Verfahren, z. Bsp. AES256 verschlüsselte 7ZIP[3] Archive zu verwenden.

(2) Bei der Softwareinstallation automatisch erzeugte bzw. vergebene Passwörter sind unverzüglich durch neue zu ersetzen.

(3) Passwörter, die nicht im Zusammenhang mit dem Anmelden (Login) einzugeben sind (anwendungsbezogene Passwörter), orientieren sich hinsichtlich der Länge der verwendeten Zeichen und der Frist für einen Passwortwechsel am Schutzbedarf der Anwendung und der zu verarbeitenden Daten. Besteht kein zusätzlicher Schutzbedarf, kann von den Vorgaben abgewichen werden.

(4) Software ist so zu gestalten bzw. grundsätzlich so zu konfigurieren, dass Benutzer nur Passwörter mit einer Mindestlänge von 8 Zeichen vergeben können. Vorgaben für anwendungsbezogene Passwörter haben den jeweiligen Schutzbedarf der Anwendung zu beachten.

(5) Fehlversuche bei der Passworteingabe sind nach technischer Möglichkeit entsprechend dem Schutzbedarf der Anwendung zu protokollieren. Die Protokolle sollen regelmäßig ausgewertet werden.

(6) Soweit möglich, ist durch softwaretechnische Maßnahmen vorzugeben, dass

1. nur Passwörter vergeben werden können, die aus der größtmöglichen Zeichenmischung von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen zusammengesetzt sind,
2. nach der vorgegebenen Frist ein Passwortwechsel erzwungen wird,
3. Benutzerkennungen, die länger als 45 Tage nicht aktiviert wurden, gesperrt werden,
4. Passwörter nicht am Bildschirm angezeigt werden,
5. Passwörter einwegverschlüsselt gespeichert werden,
6. nach 5maliger fehlerhafter Passworteingabe die Benutzerkennung gesperrt und die Systemadministration informiert wird,
7. Passwörter in Netzwerken verschlüsselt übertragen werden und
8. leicht zu erratende Passwörter nicht vergeben werden können.

(7) Ist die Sperrung der betroffenen Benutzerkennungen nach 5maliger fehlerhafter Passworteingabe nicht möglich oder sinnvoll, sind andere gleichwertige Maßnahmen zu treffen (z.B. Zeitverzögerungen zwischen den möglichen Eingabeversuchen).

(8) Bei der Auswahl von IuK-Systemen ist auf die Verfügbarkeit entsprechender Mechanismen zu achten. Sofern diese auf Ebene der Betriebssysteme oder der Anwendung nicht verfügbar sind, ist der Einsatz geeigneter Zusatz-Software erforderlich.

(9) Bei öffentlich zugänglichen Einrichtungen sind geeignete Maßnahmen zur Abwehr von Brute-Force-Methoden zum Erraten von Passwörtern, wie z. Bsp. Fail2ban[4] obligatorisch.

(10) Zum Erzeugen von Passwörtern ist das Werkzeug pwgen bzw. pwgen-win[5] oder der Passwortgenerator des Team Password Manager einzusetzen.

# Pflichten der für die Passwortverwaltung Zuständigen Mitarbeiter

(1) Auf Antrag eines Berechtigten hebt die für die Passwortverwaltung zuständige Stelle die Sperre einer Benutzerkennung auf oder neutralisiert ein Benutzerpasswort, wenn sie sich von der Identität des Berechtigten überzeugt hat. Berechtigt sind der Inhaber der betroffenen Benutzerkennung, der zur Autorisierung von Benutzern Berechtigte oder, wenn dieser nicht bestimmt wurde, der jeweilige Amtsleiter. Wurde die Sperre einer Benutzerkennung von einem zur Autorisierung von Benutzern Berechtigten bzw. dem Amtsleiter verfügt, darf die Passwortverwaltung sie nur auf dessen Auftrag hin zurücknehmen.

(2) Das Aufheben der Sperre und die Passwortneutralisierung sind revisionssicher, z. Bsp. mittels Ticketsystem zu dokumentieren, so dass nachvollziehbar ist, wer der Auftraggeber war und wie seine Berechtigung und Identität geprüft wurde.

(3) Ein von der Passwortverwaltung vergebenes Übergangspasswort (z.B. bei der Entsperrung oder der Passwortneutralisierung) ist so mitzuteilen, dass eine Kenntnisnahme durch Unbefugte vermieden wird. Zugleich ist der Empfänger des Übergangspasswortes aufzufordern, das Übergangspasswort unverzüglich zu ändern.

(4) Der Inhaber der Benutzerkennung ist von einer Passwortneutralisierung zu informieren, wenn sie nicht von ihm veranlasst wurde. Zugleich ist der Inhaber aufzufordern, das neutralisierte Passwort unverzüglich zu ändern.

1 http://keepass.info
2 http://teampasswordmanager.com
3 http://www.7-zip.org
4 http://www.fail2ban.org
5 http://pwgen-win.sourceforge.net

(5) Nicht mehr benötigte oder für einen längeren Zeitraum nicht genutzte Kennungen sind zu sperren, außer es ist für die Funktionsfähigkeit des Betriebes als solchen notwendig, dass die Kennung nicht gesperrt werden kann. Dies gilt auch für entsprechende Wartungs- und Fernwartungskennungen.

# Organisatorische Maßnahmen

(1) Soweit der Schutzbedarf der Daten und Ressourcen es erfordert, ist für die Passwörter eine angemessene Länge von mehr als 8 Stellen und eine kürzere Gültigkeitsdauer als 90 Tage festzulegen. Bei der Festlegung der angemessenen Gültigkeitsdauer sind insbesondere der potentielle Schaden zu berücksichtigen, der entstünde, wenn ein Unbefugter das Passwort über einen längeren Zeitraum nutzen würde, sowie das Risiko, das ein Unbefugter das Passwort noch längere Zeit nach Kenntnisnahme nutzen könnte.

(2) Die Einhaltung dieser Richtlinie ist durch geeignete Maßnahmen im Rahmen der Dienstaufsicht sicherzustellen.

(3) Die Beschäftigten sind entsprechend den Erfordernissen - mindestens aber einmal jährlich - über den Inhalt dieser Richtlinie zu informieren.

(4) Benutzerkennungen sollen personenbezogen vergeben werden.

(5) Werden andere Authentifizierungsmittel als Passwörter eingesetzt (z.B. Magnet-, Chipkarte, PKI), müssen sie so gehandhabt werden, dass die Benutzung durch Unbefugte ausgeschlossen ist. Soweit erforderlich, treffen die zuständigen Stellen hierzu besondere Regelungen.

# Sonstiges

Diese Anleitung findet in der managedhosting.de GmbH in Übereinstimmung mit den im BSI Massnahmenkatalog genannten Referenzdokumenten ISO 2700x nach IT-Grundschutz :

- [M 2.316] Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
- [M 2.11 ] Regelung des Passwortgebrauchs
- [M 4.14] Obligatorischer Passwortschutz unter Unix

Anwendung.

# Verantwortlichkeiten

Die Verantwortung für die Umsetzung und Einhaltung der Passwortrichtlinie liegt bei der Geschäftsführung der managedhosting.de GmbH. Die Geschäftsführung überträgt die Umsetzung der Passwortrichtlinie und die Kontrolle über deren Einhaltung an den IT- Sicherheitsbeauftragten der managedhosting.de GmbH. Die Einhaltung der IT-Sicherheitsmaßnahmen durch Mitarbeiter wird im Rahmen des Disziplinarprozesses kontrolliert.

Der IT- Sicherheitsbeauftragte der managedhosting.de GmbH nimmt seine Aufgaben in enger Zusammenarbeit mit dem Datenschutzbeauftragten der managedhosting.de GmbH wahr.

Die Geschäftsleitung der managedhosting.de GmbH kann Mitglieder der Geschäftsleitung selbst, Mitarbeiter des Unternehmens oder externe Dienstleister zum IT- Sicherheitsbeauftragten sowie Datenschutzbeauftragten bestimmen.

# Prozess zur Umsetzung der Passwortrichtlinie

Die Umsetzung der Leitlinie zur IT-Sicherheit in einen im Unternehmen laufend angewendeten IT-Sicherheitsprozess ist Gegenstand eines eigenen IT-Sicherheitskonzeptes. Dieses IT-Sicherheitskonzept orientiert sich an dem Grundschutzstandard des Bundesamtes für Informationssicherheit (BSI). Prozessverantwortlicher ist der IT-Sicherheitsbeauftragte der managedhosting.de GmbH.

# Inkrafttreten

Diese Richtlinie tritt am 01.01.2016 in Kraft.

# Weiterführende Informationen

Weiterführende Informationen und Dokumente finden Sie auch auf unserer WEB Site.

## Ergänzende Dokumente

| | |
|---|---|
| Kontakt: | https://www.managedhosting.de/contact_us/index_de.php |
| SLA: | https://www.managedhosting.de/sla |
| AGB: | https://www.managedhosting.de/agb |
| Datenschutzerklärung: | https://www.managedhosting.de/privacy |
| TOM (öffentlich): | https://www.managedhosting.de/tom |

## Ansprechpartner

Andreas Wolske

E-Mail: andreas.wolske@managedhosting.de

Telefon: +49 800 6737877

Mobil: +49 151 21258008

managedhosting.de GmbH
Friedrichstr. 191
10117 Berlin