ABl 13/2020, S. 468-474

# Passwortrichtlinie

## 1 Einleitung

Passwörter und Benutzerkonten werden als grundlegender Authentifizierungsmechanismus in IT- und Telekommunikationssystemen eingesetzt und bieten den Basisschutz für die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen auf den Systemen und in den Anwendungen. Diese Richtlinie beschreibt verbindlich die Mindestanforderungen an die Qualität von Passwörtern und die Regeln im Umgang mit Passwörtern und Benutzerkonten im Bistum Augsburg.

## 2 Definitionen

Diese Richtlinie ist im Rahmen der technischen Möglichkeiten auf alle IT- und Telekommunikationssysteme anzuwenden, die durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung, oder Veränderung der auf ihnen gespeicherten Daten, geschützt werden sollen. Dazu gehören unter anderem:

- **Systemsoftware**

  wie Microsoft Windows, Linux, Cisco IOS, BIOS, Firmware etc.

- **Applikationen**

  wie Bizagi, Intentio, ELO etc.

- **Standardsoftware**

  wie Datev, Helpline, etc.

- **systemnahe Softwarebestandteile**
  wie Tools, Utilities, Citrix, VMware, Secure PIM, AV-Scanner etc.

Diese Richtlinie legt die Mindestanforderungen fest. Ausnahmen müssen durch die Stabsstelle Informationssicherheit genehmigt werden.

## 3 Allgemeiner Umgang mit Passwörtern

Für den verantwortungsvollen Umgang mit Passwörtern beachten Sie folgende Festlegungen:

- **Passwörter müssen geheim gehalten werden und dürfen nur dem Benutzer persönlich bekannt sein.**
- Passwörter dürfen nicht weitergegeben werden.
- 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 Eingabe ist darauf zu achten, dass sie nicht von Dritten eingesehen werden können.
- Ein Passwort muss sofort gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.
- Passwörter dürfen nur verschlüsselt in Dateien abgelegt werden.
- Bei der physischen Hinterlegung muss das Passwort in einem versiegelten Umschlag sicher aufbewahrt werden (z.B. Tresor).
- Voreingestellte Passwörter (Initialpasswörter) sind umgehend durch ein persönliches Passwort zu ersetzen.

- Verwenden Sie Passwörter, die Sie im privaten Umfeld nutzen, nicht im beruflichen Bereich.
- Passwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses verwendet werden, z.B. in einer Funktionstaste oder im Passwortspeicher eines Internet-Browsers.

## 4 Vorgaben für Passwörter von normalen Benutzerkonten

Normale Benutzerkonten (Anwenderkonten) haben keine administrativen Rechte in den IT- und TK-Systemen. Diese Konten werden für die normalen Arbeiten der Mitarbeiter in den Anwendungen (Applikation, Standardsoftware, Systemsoftware) zu Verrichtung ihrer täglichen Aufgaben benutzt.

Um eine Mindestqualität der Passwörter zu gewährleisten, sind die folgenden Einstellungen – soweit technisch möglich – systemseitig vorzunehmen.

| Anforderung | Vorgabe |
|---|---|
| **Mindestlänge des Passworts** | 8 Zeichen |
| **Komplexitätsanforderung** | Großschreibung<br>Kleinschreibung<br>Sonderzeichen<br>Zahlen<br>**Mindestens 3 dieser 4** Anforderungen müssen erfüllt sein |

**Alle Mitarbeiter müssen diese Vorgabe an die Qualität ihres persönlichen Passworts beachten und umsetzen**, soweit es die Anwendung (Applikation, Standardsoftware, Systemsoftware) zulässt.

Neben den formalen Anforderungen an den Aufbau eines sicheren Passworts sind systemseitig – soweit technisch möglich – weitere global geltende Parameter einzustellen.

| Anforderung | Vorgabe |
|---|---|
| **Änderungsintervall** | Sollte der Verdacht bestehen, dass das Passwort unbefugten Dritten bekannt sein könnte, ist es zwingend sofort zu ändern.[1] |
| **Anzahl falscher Anmelde-versuche** | 10 Versuche bis zum Sperren der Kennung des Benutzers (manuelles Entsperren durch einen Administrator / Service Desk notwendig) |
| **Alternativ dazu:** | 5 Versuche bis zum Sperren der Kennung des Benutzers und automatisches Entsperren durch das System / die Anwendung nach 30 Minuten |
| **Passwort Historie** | 10 |
| **Minimales Passwortalter** | 1 Tag[2] |

## 5 Vorgaben für Administratoren und Entwickler

- Die bei einer Softwareinstallation vom Hersteller vorgegebenen Passwörter (Standardpasswörter) sind unverzüglich zu ändern.
- Bei Programmen (Anwendungen), die eine Authentifizierung unterstützen oder voraussetzen, ist die Methode Single-Sign-On. sofern technisch möglich, einzusetzen.
- Fehlversuche bei der Passworteingabe sind mindestens auf geschäftskritischen und sicherheitsrelevanten Systemen zu protokollieren. Die Protokolle sind regelmäßig auszuwerten.
- Es ist durch geeignete Maßnahmen sicherzustellen, dass auch in einem Notfall / Krisenfall ein Zugriff auf die Passwörter möglich ist. Änderungen sind entsprechend einzupflegen, damit die Passwortliste im Ernstfall auf dem aktuellen Stand ist.
- Durch Konfigurationsanforderungen müssen folgende Anforderungen sichergestellt werden:
  - o Passwörter müssen den Komplexitätsanforderungen entsprechen.
  - o Passwörter dürfen am Bildschirm nicht in Klartext sichtbar sein.
  - o Passwörter müssen verschlüsselt gespeichert werden.
  - o Nach 10-maliger fehlerhafter Eingabe muss die Benutzerkennung gesperrt und die Systemadministration informiert werden.
  - o Passwörter müssen in Netzwerken verschlüsselt übertragen werden.

[1] Das BSI rät im Kapitel zur Regelung des Passwortgebrauchs, das Kennwort zu ändern, wenn es in fremde Hände geraten sein könnte. Die dort bisher aufgeführte Verpflichtung, das Passwort regelmäßig zu ändern, wurde aufgehoben.

[2] Um die Passworthistorie sinnvoll zu nutzen, sollte auch die Einstellung „Minimales Passwortalter“ konfiguriert werden. So wird vermieden, dass Passwörter in kurzer Zeit mehrmals geändert werden. Mit dieser Kombination ist es dem Benutzer nicht möglich, versehentlich oder absichtlich alte Passwörter erneut zu verwenden.

## 6 Vorgaben für hochprivilegierte Accounts

Diese Einstellungen sind für Benutzerkennungen mit weitreichenden Rechten im System oder der Anwendung wie z.B. Systemkonten, Service Accounts und administrative Accounts (Systemverwalterkonto) vorzunehmen.

**Systemkonten** sind Spezialkennungen für technische Abläufe wie zum Beispiel Transferkennungen zwischen IT-Systemen. Sie werden in aller Regel einmalig mit einem Passwort belegt, das nicht mehr geändert wird. Eine Anmeldung als interaktiver Benutzer ist mit diesen Kennungen von vornherein nicht möglich oder wurde konfigurationsseitig unterbunden.

**Service Accounts** werden für die technische Unterstützung von externen Dienstleistern verwendet. Sie werden bei Unterstützungsleistungen freigeschaltet und nach Erledigung der Arbeiten wieder gesperrt.

**Administrative Accounts** (Systemverwalterkonten) umfassen alle lokalen und domänengebundenen Benutzerkennungen sowie alle hochprivilegierten Kennungen mit Rechten zur Wartung der IT- und TK-Systeme (root, administrator, sys, dbadmin, sysadm, ...).

| Anforderung | Vorgabe |
|---|---|
| **Mindestlänge des Passwortes** | 16 Zeichen |
| **Komplexitätsanforderung** | Großschreibung Kleinschreibung<br>mindestens 2 Sonderzeichen[3]<br>mindestens 2 Zahlen |
| **Passwort Historie** | 10 Passworte |
| **Minimales Passwortalter** | 1 Tag |
| **Maximales Passwortalter** | 90 Tage |
| **Anzahl zulässiger fehlgeschlagener Anmeldeversuche** | 5 |
| **Sperrung nach Überschreitung zulässiger Fehlversuche** | 30 Minuten |
| **Entsperrung des Zählers fehlgeschlagener zulässiger Anmeldeversuche** | 30 Minuten |

Sofern interne oder externe Mitarbeiter, die im Bereich der IT- Systemadministration arbeiten oder zur Durchführung ihrer Tätigkeit administrative Benutzerkennungen verwenden, das Unternehmen verlassen oder ihre Tätigkeit dahingehend ändern, dass sie diese administrativen Kennungen nicht mehr benötigen, ist eine unverzügliche Änderung der ihnen bekannten administrativen Passwörter durchzuführen. Bei sicherheitskritischen Systemen (z.B. Firewalls) ist die Änderung der Passwörter ebenfalls verpflichtend und unverzüglich mit höchster Priorität umzusetzen.

Der Rechteentzug ist dem Prozess dem Berechtigungsantragsprozess entsprechend zu dokumentieren. Jede Änderung ist in die Notfalldokumentation einzupflegen.

[3] Können keine Sonderzeichen verwendet werden, muss die Länge des Passworts auf 20 Zeichen verlängert werden. Die Sonderzeichen entfallen dann.

## 7 Vorgaben für Smartphones (BYOD, PIM)

Die auf den Smartphones durch die IT installierten Apps (z.B. Secure PIM) sind mit einem Passwort zu versehen. Es gelten folgende Vorgaben:

| Anforderung | Vorgabe |
|---|---|
| Mindestlänge des Passworts | 8 Zeichen |
| **Komplexitätsanforderung** | Großschreibung Kleinschreibung Zahlen<br>Mindestens **2 dieser 3** Anforderungen müssen erfüllt sein |
| **Änderungsintervall** | Sollte der Verdacht bestehen, dass das Passwort unbefugten Dritten bekannt sein könnte, ist es umgehend zu ändern. |
| **Biometrie** | Das Passwort kann durch ein biometrisches Passwort (Gesichtserkennung, Fingerabdruck-scanner) ergänzt werden. |
| **Anzahl falscher Anmeldever-suche** | 5 Versuche bis zum Sperren der Kennung des Benutzers (manuelles Entsperren durch einen Administrator notwendig) |

## 8 Mehrfaktorauthentifizierung (MFA)

Eine sicherere Art, Zugänge zu Systemen abzusichern, ist die Zwei-wege-Authentifizierung (auch Multi Factor Authentication). Diese Art der Authentifizierung ist bei allen Systemen, die Zugänge aus dem Internet auf IT-Systeme ermöglichen (z.B. Citrix Zugänge), vorgeschrieben, soweit das technisch möglich ist. Bei kritischen Systemen, auf denen streng vertrauliche Informationen (z.B. Datenschutzklasse III) verarbeitet oder gespeichert werden, ist diese Art der Authentifizierung in der Sicherheitsarchitektur mit zu betrachten und als Authentifizierung in Erwägung zu ziehen, sofern technisch möglich, wirtschaftlich und praktikabel.

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

## 9 Anonyme Benutzerkennungen

Anonyme Benutzerkennungen sind regulär zu vermeiden. Benutzerkennungen müssen personenbezogen vergeben werden, d.h. einem Benutzer zweifelsfrei zuzuordnen sein. Ausnahmen sind mit dem Leiter der Stabsstelle Informationssicherheit abzustimmen.

Die einzige reguläre Ausnahme bilden Systemkennungen und Spezialkennungen für technische Abläufe.

## 10 Behandlung von Ausnahmen

Die Passwortrichtlinie wird in allen IT-Systemen angewendet, in denen es technisch und organisatorisch möglich ist.

Ist die Umsetzung nicht möglich, beispielsweise, weil die Anwendung die Einstellung von Passwortanforderungen nicht in vollem Maße zulässt, so ist zu prüfen, ob weitere technische oder organisatorische Maßnahmen zur Sicherung des Zugangs

auf die Anwendungen implementiert werden können, wie z.B.

- Verwendung von biometrischen Authentifizierungsmethoden
- Mehr-Faktor-Authentifizierung.

Sollten technische oder organisatorische Notwendigkeiten erfordern, dass von einer in diesem Dokument aufgeführten Vorgabe abgewichen werden soll oder muss, so ist der Leiter der Stabsstelle Informationssicherheit in den Entscheidungsprozess für die Erteilung einer Ausnahmegenehmigung mit einzubeziehen. Die Ausnahme ist entsprechend zu dokumentieren.

## 11 Schlussbemerkung / Dokumentation

Diese Richtlinie wird in regelmäßigen Abständen (mindestens alle 2 Jahre) geprüft und aktualisiert. Bei Änderungswünschen senden Sie bitte eine E-Mail an informationssicherheit@bistum-augsburg.de.

## 12 Inkrafttreten

Diese Richtlinie tritt zum 01.12.2020 in Kraft.