I-06f Passwortrichtlinie Mitarbeiter

Inhalt

Dieses Dokument regelt die grundsätzliche Gestaltung und Handhabung von Passwörtern, die beispielsweise zur Verschlüsselung von Daten oder zur Authentifizierung berechtigter Mitarbeiter/-innen sowohl im Netzwerk, Anwendungen und Fachverfahren des Landratsamtes Ebersberg als auch Internetdiensten eingesetzt werden. Sie ist auf alle IT-Systeme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.

Dokumenteninformation

Titel des Dokuments				**Vertraulichkeitsstatus**	
I-06f Passwortrichtlinie Mitarbeiter				Intern	
Version	**Datum**	**Änderungen**	**Autor**	**Status**	**Freigabe**
1.0	26.10.2023	Erstellung des Dokuments basierend auf SiKoSH_Richtlinie-Passwortrichtlinie-vs_1_9 (IT-VSH)	K. della Peruta	Revision IS-Team	
1.1	20.02.2024	7. Komplexität und Lebensdauer von Passwörtern Nach (maximal) 5 erfolglosen Authentifizierungsversuchen ist ein Benutzerkonto zu sperren. Benutzerkonen werden nach 30 Minuten automatisch entsperrt.	D. Jansen	Revision IS-Team	
1.2	04.04.2024	Kürzung des Punktes PINs und Codes; Generelle Überarbeitung; automatische Freischaltung nach 30 Minuten eingetragen. Kennwortsätze aktualisiert.	M. Blabsreiter	Revision IS-Team	
1.3	05.04.2024	Anpassung Übermittlung Kennwörter; IT statt IT-Abteilung;	M. Blabsreiter	Revision IS-Team	
1.4	05.04.2024	Rechtschreib- und Grammatikprüfung; Verlinkung Anleitungen KeePass und Passwortleitfaden; Neutralsetzung ISB und DSB;	M. Blabsreiter	Final	ISB/ 08.04.2024

Inhaltsverzeichnis

1 Geheimhaltung von Passwörtern

Passwörter sind geheim zu halten.

Sie sind verdeckt einzugeben und dürfen insbesondere nicht

- auf Funktionstasten hinterlegt werden
- unverschlüsselt abgelegt/abgespeichert werden
- offen zugänglich auf Rechnern oder anderen Informationsträgern (z.B. Papier) gespeichert werden.

Passwörter von personalisierten Benutzerkonten dürfen in keinem Fall **– auch nicht an Administratoren / in oder zu Vertretungszwecken –** weitergegeben werden. Vertretungen sind durch ein Berechtigungsmanagement zu regeln.

2 Personalisierte Benutzerkonten

Personalisierte Benutzerkonten müssen über einen eindeutigen Namen einer natürlichen Person zugeordnet sein.

3 Umgang mit nicht personalisierten Benutzerkonten

Systemkonten dürfen nur aus **zwingenden technischen Gründen** eingerichtet werden, wenn die Funktionalität des Systems mit anderen Mitteln in wirtschaftlich vertretbarem Umfang und unter nachvollziehbarer Risikobewertung anders nicht herstellbar ist.

Passwörter von **nicht personalisierten Benutzerkonten** sind verschlossen und sicher (vornehmlich in einem Tresor), noch besser in einem **Passwortmanager** zu hinterlegen. Es ist zu dokumentieren, wem und ggf. unter welchen Bedingungen das Passwort ausgehändigt werden kann:

Passwort	Berechtigte(r)	Voraussetzungen

Tabelle 1 Beispiel Hinterlegung des Passwortes

4 Komplexität und Lebensdauer von Passwörtern

Unsere Passwortrichtlinie beinhaltet generell folgende komplexe Regeln:

- mindestens zwölf Zeichen lang
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen (# $ & @ € ! ? etc.)

Da alle Passwörter den komplexen Vorgaben folgen, wird auf eine regelmäßige Änderung von Passwörtern verzichtet.

Zusätzliche Regelungen:

1. Benutzerkennungen mit besonderen Rechten und Aufgaben (z.B. Systemverwaltung, Sicherheitsfunktionen oder Anwendungen mit sensiblen Daten) sind mit besonders starken Passwörtern zu schützen, die mindestens 20 Zeichen umfassen.

2. Einstiegs- und Übergangspasswörter sind unverzüglich durch eigene Passwörter zu ersetzen.

3. Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Das sind insbesondere solche mit:
    a. Zeichenwiederholungen
    b. Zahlen und Daten aus dem Lebensbereich des Benutzers (Geburtsdatum, Telefonnummern)
    c. Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen
    d. einfache Ziffern- und Buchstabenkombinationen
    e. Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden, Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter).
    f. Für Zugänge zu externen Anwendungen (Cloud-Lösungen, Webanwendungen) müssen unterschiedliche Passwörter verwendet werden.

4. Nach (maximal) **fünf** erfolglosen Authentifizierungsversuchen wird ein Benutzerkonto automatisch gesperrt. Diese Konten werden nach **30 Minuten** automatisch wieder vom System entsperrt.

5. Passwortsätze haben sich bewährt, sie sind leicht zu merken und dennoch lang und komplex genug um der Passwortrichtline zu entsprechen. Die einzelnen Wörter dürfen nicht in Abhängigkeit zueinanderstehen (z.B. Am1.JanuaristNeujahr.). Es müssen komplett verschiedene Wörter kombiniert werden (z.B. 19@Kiefernwald-Boersencrash€Korallenriff).

5 Passwortmanager

Die Mitarbeiter sind angehalten Passwörter mit dem Passwortmanager KeePass zu verwalten und zu generieren. Der KeePass Passwortmanager ist auf jedem PC und Laptop im Landratsamt Ebersberg installiert und kann vom ersten Tag an genutzt werden. Weitere Informationen sind in der Anwenderhilfe zu finden:

https://doku.lra-ebe.bayern.de/display/Hilfe/Einrichtung+des+Passwort-Managers

https://doku.lra-ebe.bayern.de/pages/viewpage.action?pageId=106070574

6 Verluste oder Kompromittierung von Passwörtern

Ist eine unbeabsichtigte oder unautorisierte **Offenlegung des Passworts** erfolgt oder wird diese vermutet, ist das Passwort **unverzüglich zu ändern**. In diesem Fall ist die/der ISB (Informationssicherheitsbeauftragte), die IT und ggf. die/der DSB (Datenschutzbeauftragte) unverzüglich zu informieren.

7 Übermittlung von Passwörtern

Die elektronische Übermittlung von Zugangsdaten, wie Passwort und Benutzerkennung, an Personen bzw. innerhalb von vernetzten Systemen, darf **ausschließlich** über den zweiten Kommunikationskanal übermittelt werden**. Passwörter** und **Benutzerkennungen** dürfen zudem nicht zusammen übermittelt werden. So kann z.B. die Benutzerkennung per E-Mail und das zugehörige Kennwort per Telefon, SMS, verschlüsselter Nachricht oder in Briefform übermittelt werden.

8 Nutzung von PINs / Codes bei Apple Geräten

Zur Sicherung von mobilen Endgeräten (z.B. **Smartphones, Tablets**, etc.) ist ein Code zu verwenden. Die Länge des PINs/ Codes darf **5 Zeichen** nicht unterschreiten. SIM-Karten werden durch eine PIN (Persönliche Identifikationsnummer) gesichert. Diese muss zwingend **vierstellig** sein.

9 Nutzung alternativen Authentisierungsverfahren (Biometrie)

Eine biometrische Erkennung wird an den Apple Geräten (iPhones und iPads) im Landratsamt eingesetzt (FaceID und TouchID).

10 Ausnahmen

Ausnahmen von dieser Passwortrichtlinie sind nur nach Genehmigung durch die/den ISB (Informationssicherheitsbeauftragte(n)) und ggf. die/den DSB (Datenschutzbeauftragte(n)) möglich. Der Antrag hat schriftlich begründet zu erfolgen.

Schlussbestimmung / Inkrafttreten

Diese Richtlinie tritt mit dem Tag der Veröffentlichung (im Intranet) in Kraft.