Arbeitsrichtlinie Kennwörter

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Kennwörter
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	14.10.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	April 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	14.10.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	19.05.2020	Redaktionelle Änderungen und Aktualisierung der Ausnahmen (Kapitel 4.4)	Daniel Fürdauer
21.0	29.04.2021	Anpassung der Passwortlänge und des Passwortablaufs in Anlehnung an die Empfehlung des BSI. Erhöhung der Versuche bis zur Automatischen Sperre, um versehentliche Sperren zu reduzieren. Aufnahme einer Ausnahmeregelung für Active-Directory-Benutzer. Ausnahme: Speichern von Kennwörtern in Browsern; Redaktionelle Änderungen	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. ZIELSETZUNG

Kennwörter werden im großen Umfang zur Authentisierung verwendet. In vielen Fällen sind Kennwörter die einzige Authentisierung und damit von entscheidender Bedeutung für die Informationssicherheit der VAV.
Ziel dieser Arbeitsrichtlinie ist es, die Vorgaben für einen sicheren Einsatz und Umgang mit Kennwörtern zu definieren.

2. ALLGEMEINE ANFORDERUNGEN

2.1. Anwendungsbereich

Kennwörter werden zwingend für alle Zugriffe auf die IT-Systeme der VAV benötigt. Der Passwortschutz eines IT-Systems soll gewährleisten, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen. Unmittelbar nach dem Einschalten des IT-Systems muss der Berechtigungsnachweis erfolgen. Kann der Benutzer die erforderliche Berechtigung nicht nachweisen, so verhindert der Passwortschutz den Zugriff auf das IT-System.

2.2. Generelle Anforderungen beim Einsatz

Es gelten die folgenden generellen Anforderungen an jegliche Kennwortnutzung bei der VAV

- Jeder Benutzer muss individuelle Kennwörter benutzen und muss diese auch selbst verändern können. Ein Account- oder Kennwort-Sharing (Mehrfachnutzung / Kennworthinterlegung) ist untersagt.
- Nach der Installation bzw. der Neueinrichtung von Benutzern müssen Initialkennwörter durch den Vorgesetzten auf sichere Art übergeben werden. Initiale Kennwörter sind den Benutzern auf sichere Art zu übergeben und unterliegen den gleichen Anforderungen wie die durch die Benutzer verwendeten Kennwörter. Das Initialkennwort muss im Rahmen der Erstanmeldung systemseitig geändert werden. Es ist ein Einmalkennwort.
- Kennwörter müssen Mindestanforderungen an die Mindestlänge und Komplexität erfüllen. Dies gilt auch, wenn Kennwörter automatisch generiert werden.
- Es ist ein regelmäßiger Kennwortwechsel durch den Benutzer durchzuführen.
- Beim Ändern seines Kennworts muss ein Benutzer sein altes Passwort zur Bestätigung eingeben.
- Bei der Eingabe darf das Kennwort auf dem Bildschirm nicht im Klartext angezeigt werden.
- Kennwörter dürfen grundsätzlich nicht von den Benutzern in Anmeldemasken gespeichert werden, entsprechende Optionen sind zu deaktivieren (Ausnahme: In Internet-Browsern)
- Die Ablage von Kennwörtern im System (ins. Passwortmanager) durch die Administratoren muss zugriffsgesichert erfolgen, z.B. mittels Einwegverschlüsselung.
- Voreingestellte Kennwörter, z.B. von Herstellern, sind vor Inbetriebnahme zu ändern.
- Kennwörter dürfen nicht als Teil eines automatischen Anmeldeprozesses verwendet werden, beispielsweise in einer Makro- oder Funktionstaste.
- Wenn der Verdacht besteht, dass die eigenen Zugangsmittel unberechtigt Dritten offenbart wurden, sind das Kennwort umgehend zu ändern und die Stabstelle Datenschutz und Informationssicherheit mit eindeutigem Hinweis auf einen möglichen unberechtigten Zugriff zu informieren.

2.3. Kennworthinterlegung

Kennwörter sind streng vertraulich. Sie dürfen auch im Vertretungsfall nicht an die Vertretung weitergegeben werden.
Administrative Kennwörter für IT-Systeme und technische Benutzer sind an einer zentralen Stelle, beispielsweise in einem Kennwort-Safe der zuständigen Administratoren, zugriffsgeschützt zu hinterlegen.

3. VERGABE, ÄNDERUNG UND SPERRE

3.1. Zurücksetzung

Ein Zurücksetzen von Kennwörtern ist erforderlich, wenn ein Benutzer ein Kennwort vergessen hat. Es muss dabei verhindert werden, dass sich Unberechtigte durch unzureichende Prüfungen Berechtigungen verschaffen können.
Für die Zurücksetzung von Kennwörtern ist der IT Support zu kontaktieren.
Bei der Verwendung von E-Mails als Faktor für Passwortzurücksetzungen z. B. in Portalen dürfen nur vorab bekannte E-Mail-Adressen verwendet werden. Versendete Zurücksetzungspasswörter bzw. -Tokens dürfen nur temporär gültig sein.
Anwender müssen über eine systemseitig durchgeführte Passwortzurücksetzung z. B. durch Initiierung durch den Vorgesetzten informiert werden. Die Benachrichtigung sollte Meta-Informationen, wie Zeitpunkt, IP-Adresse und Anfrage-ID, enthalten.

3.2. Anforderungen an das Kennwort

Für die Auswahl von Kennwörtern gelten die folgenden Anforderungen bei den Active Directory-Passwörtern:

REGEL	WERT
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Minimale Kennwortlänge	12 Zeichen
Maximales Kennwortalter	365 Tage
Minimales Kennwortalter	2 Tage
Kennwortchronik erzwingen/ gespeicherte Kennwörter	24 gespeicherte Kennwörter
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert

Tabelle 1: Kennwortvorgaben

3.2.1. Komplexitätsvoraussetzungen

1. Kennwörter enthalten möglicherweise nicht den sAMAccountName-Wert (Kontoname) des Benutzers oder gesamten DisplayName (vollständiger Name-Wert). Bei beiden Prüfungen wird die Groß-/Kleinschreibung nicht berücksichtigt.
   Das SamAccountName wird in seiner Gesamtheit nur überprüft, um festzustellen, ob es Teil des Kennworts ist. Wenn die sAMAccountName kleiner als drei Zeichen lang ist, wird diese Überprüfung übersprungen. Der DisplayName wird für Trennzeichen analysiert: Kommas, Punkte, Striche oder Bindestriche, Unterstriche, Leerzeichen, Nummernzeichen und Tabstopps. Wenn eines dieser Trennzeichen gefunden wird, wird der DisplayName geteilt, und alle analysierten Abschnitte (Tokens) werden bestätigt, dass Sie nicht im Kennwort

enthalten sind. Token, die kleiner als drei Zeichen sind, werden ignoriert, und Teilzeichenfolgen der Token werden nicht überprüft. Beispielsweise wird der Name "Erin M. Hagens" in drei Token aufgeteilt: "Erin", "M" und "Hagens". Da das zweite Token nur ein Zeichen lang ist, wird es ignoriert. Daher konnte dieser Benutzer nicht über ein Kennwort verfügen, das "Erin" oder "Hagens" als Teilzeichenfolge an einer beliebigen Stelle im Kennwort enthielt.

2. Das Kennwort enthält Zeichen aus drei der folgenden Kategorien:
    - Großbuchstaben europäischer Sprachen (A bis Z, mit diakritischen Zeichen, griechischen und kyrillischen Zeichen)
    - Kleinbuchstaben europäischer Sprachen (a bis z, Sharp-s, mit diakritischen Zeichen, griechischen und kyrillischen Zeichen)
    - Basis 10 Ziffern (0 bis 9)
    - Nicht alphanumerische Zeichen (Sonderzeichen): (~! @ # $% ^& * _-+ = ' | \ \ (){}\ []:; '" <>,.? /) Währungssymbole wie Euro oder Britisches Pfund werden nicht als Sonderzeichen für diese Richtlinieneinstellung gezählt.
    - Ein beliebiges Unicode-Zeichen, das als Alphabetisches Zeichen kategorisiert ist, aber kein groß-oder Kleinbuchstaben ist. Dazu gehören Unicode-Zeichen aus asiatischen Sprachen.

3.3. Automatische Sperre

Es ist eine automatische Sperre des Accounts bei einer mehrmaligen Falsch-Eingabe des Kennworts vorzusehen.
Wenn der Domain-Account (Windows, Outlook, Citrix) aufgrund von einer 5-maligen Falsch-Eingabe des Kennworts gesperrt wurde, ist der IT Support zu kontaktieren. Bei einer 4-maligen Falsch-Eingabe des Kennworts, vergehen 30 Minuten bis wieder 5 Versuche zur Verfügung stehen.

3.4. Ausnahmen bei Active Directory-Benutzern

Der IT-Support dokumentiert alle Ausnahmen bei Active Directory-Konten (3.2) in einer Liste. Ausnahmen mit einem geringen Risiko sind von dem Informationssicherheitsbeauftragten zu genehmigen und Ausnahmen mit einem mittleren oder hohen Risiko sind vom Vorstand zu genehmigen. Der Informationssicherheitsbeauftragte bewertet das Risiko der jeweiligen Ausnahme. Der Informationssicherheitsbeauftragte meldet die Liste aller Ausnahmen bei Active Directory-Benutzern vierteljährlich an den Vorstand im Rahmen der regelmäßigen Berichterstattung der Richtlinie Exception Handling.
Active-Directory-Benutzer mit nicht genehmigten Ausnahmen sind umgehend von dem IT-Support zu sperren.

Im Rahmen des Regelprozesses zum Umgang mit Arbeitsrichtlinien in der IT prüft der IT-Support die Umsetzung und erstellt erneut eine Dokumentation aller Ausnahmen und diese müssen erneut entsprechend obiger Vorgehensweise behandelt werden.

4. AUSNAHMEN

Ausnahmen z. B. aufgrund von technischen Restriktionen sind individuell mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen.

4.1. Kundenportale

Bei den Kundenportalen handelt es sich in der Regel um Zugriffmöglichkeiten auf persönliche Kundeninformationen. Folgende Abweichungen sind zugelassen:

- Maximale Länge: Zur Vermeidung von DoS-Attacken auf zum Beispiel 512 Zeichen beschränken
- Ungültige Zeichen: Keine Vorgabe
- Erforderliche Zeichen: Zahlen, Buchstaben (Groß- / Kleinschreibung), Sonderzeichen
- Kennwortablauf: Keine Vorgabe
- Eine Kennwortzurücksetzung muss der Kunde selbst durchführen können

4.2. Technische (Service) Accounts

Technische Accounts bei Windows-, Linuxserver oder aktiven Netzkomponenten starten Dienste, Services oder werden zur Maschinen-zu-Maschinenkommunikation benötigt. Folgende Abweichungen sind zugelassen bzw. umzusetzen:

- Minimale Länge: 12 Zeichen
- Ungültige Zeichen: Keine Vorgabe
- Erforderliche Zeichen: Zahlen, Buchstaben (Groß- / Kleinschreibung), Sonderzeichen
- Kennwortablauf: Keine Vorgabe
- Das Kennwort ist immer zu ändern, wenn ein Mitarbeiter, der das Kennwort kennt, das Unternehmen verlässt oder die Abteilung wechselt und bei Missbrauchsverdacht.
- Das Passwort eines technischen Users darf zwischen Test und Produktionsebene nicht identisch sein

4.3. Privileged Accounts

Die Nutzung von Privileged Accounts erlaubt einem Benutzer Anwendungen mit erhöhten Rechten auszuführen, als auch ein System zu administrieren. Die Kennwörter müssen folgende Eigenschaften aufweisen:

- Maximale Länge: Zur Vermeidung von DoS Attacken auf 512 Zeichen beschränken
- Minimale Länge: 12 Zeichen
- Ungültige Zeichen: Keine Vorgabe
- Erforderliche Zeichen: Zahlen, Buchstaben (Groß- / Kleinschreibung), Sonderzeichen

4.4. Technische Voraussetzung / Nutzbarkeit

Es gibt Geräte und Systeme, die aufgrund ihrer technischen Voraussetzungen die Anforderung der Richtlinie nicht umsetzen können oder die Nutzbarkeit übermäßig einschränken.

4.4.1. Smartphone

Ausnahmen für den Systemzugang, nicht aber für die Domain-Zugangsdaten:

- Minimale Länge: 8 Zeichen
- Ungültige Zeichen: Keine Vorgabe
- Erforderliche Zeichen: Zahlen
- Kennwortablauf: Keine Vorgabe
- Eine Kennwortzurücksetzung muss der Mitarbeiter selbst durchführen können
- Alternativ ist die Verwendung eines Erkennungsverfahrens für ein geeignetes, biometrisches Merkmal zulässig

4.4.2. Tablets

Ausnahmen für den Systemzugang, nicht aber für die Domain-Zugangsdaten:

- Minimale Länge: 8 Zeichen
- Ungültige Zeichen: Keine Vorgabe
- Erforderliche Zeichen: Zahlen
- Kennwortablauf: Keine Vorgabe
- Eine Kennwortzurücksetzung muss der Mitarbeiter selbst durchführen können
- Alternativ ist die Verwendung eines Erkennungsverfahrens für ein geeignetes, biometrisches Merkmal zulässig

4.4.3. Online-Systeme

Bei Online-Systemen, wie zum Beispiel dem Newsletter-Tool, Content-Management-Systemen und Datenübertragungs-Tools., sind die entsprechenden Kennwort-Einschränkungen zu beachten.
Es sind allerdings die folgenden Vorgaben zu beachten:

- Minimale Länge: 12 Zeichen
- Ungültige Zeichen: Keine Vorgabe
- Erforderliche Zeichen: Zahlen, Buchstaben (Groß-/Kleinschreibung), Sonderzeichen
- Kennwortablauf: Keine Vorgabe
- Das Kennwort ist immer zu ändern, wenn ein Mitarbeiter, der das Kennwort kennt, das Unternehmen verlässt oder die Abteilung wechselt und bei Missbrauchsverdacht.
- Das Passwort eines technischen Users darf zwischen Test und Produktionsebene nicht identisch sein

4.4.4. Sonstige Systeme

Bei Systemen der VAV, insbesondere Programmen, mit technischen Einschränkungen ist darauf zu achten, dass der Zugriff auf diese nur nach der Windows/Citrix-Anmeldung möglich ist und die Informationen auf diese Art geschützt sind.

5. ANLAGE: EINSTELLUNGEN DOMAIN-POLICY

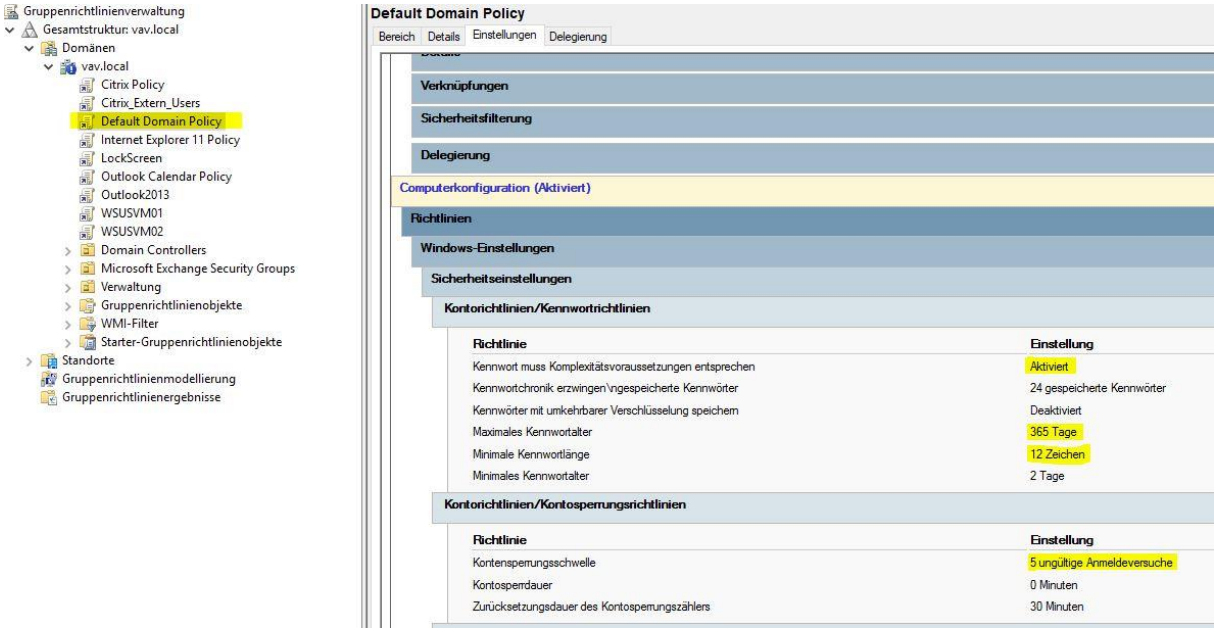

Abbildung 1: Kennwortvorgaben