Arbeitsrichtlinie Zugangssteuerung

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.1

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Zugangssteuerung
Version	21.1
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	23.10.2019
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	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	23.10.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Redaktionelle Änderungen und Klarstellung bestehender Regelungen in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 20.1.	Daniel Fürdauer
21.0	17.11.2021	In Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0: Ergänzung im Kapitel 4.1 zu Multifaktorauthentisierung; Redaktionelle Änderungen/Klarstellungen	Daniel Fürdauer
21.1	23.12.2021	Änderung der Erstellungsfrist von Rollen- und Berechtigungskonzepten in Kapitel 1.2. auf 31.12.2022	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. EINLEITUNG

1.1. Zielsetzung

Diese Arbeitsrichtlinie dient dazu, einheitliche Vorgaben für die Definition, Vergabe und Administration von Benutzern[1] und deren Rollen und Berechtigungen zu schaffen, um

- versehentliche wie absichtliche Manipulationen der Unternehmens- und Kundendaten zu verhindern,
- sicherzustellen, dass nur qualifiziertes Personal Daten eingeben, ändern oder löschen kann,
- sicherzustellen, dass die Zugriffe prüfbar sind,
- vertrauliche Informationen vor unberechtigter Kenntnisnahme zu schützen,
- die gesetzlichen Anforderungen hinsichtlich des Datenschutzes zu erfüllen,
- die Berechtigungsverfahren transparent und nachvollziehbar zu halten und
- das interne Kontrollsystem umzusetzen.

1.2. Anwendungsbereich

Der Anwendungsbereich dieser Regelung erstreckt sich über Anwendungen, Betriebssysteme und Datenbanken losgelöst von der Frage, ob es sich um ein Test- oder Produktivsystem handelt oder nicht. Testsysteme sind ausgenommen, soweit sie lediglich synthetische oder anonymisierte Daten enthalten.
Die Anforderungen gelten für alle Rollen und Berechtigungen.
Diese Richtlinie gilt zudem für Dateilaufwerke.
Rollen- und Berechtigungskonzepte sind bis 31.12.2022 zu erstellen.

2. ALLGEMEINE ANFORDERUNGEN

2.1. Need-to-Know-Prinzip

Jeder Benutzer (User) darf nur die Berechtigungen besitzen, die für die jeweilige Aufgabe benötigt werden (sog. Need-to-Know-Prinzip). Bei der Bündelung von Berechtigungen zu Rollen muss das Minimalprinzip ebenfalls beachtet werden.

2.2. Funktionstrennung

Die Rechte-/ Funktionstrennung (auch "Segregation of Duties" genannt) ist ein wesentlicher Aspekt im Berechtigungsmanagement, der stets beachtet und im Rahmen des Rollen- und Berechtigungskonzepts abgebildet werden muss. Das bedeutet, dass sich auszuschließende Rechte auf Rollenebene unterbunden werden müssen.

[1] Benutzer sind alle Mitarbeiter der VAV, inklusive Zeitarbeitskräften, sowie Dritte, welche auf Anwendungen, Betriebssysteme und Datenbanken zugreifen können.

2.3. Nachvollziehbarkeit

Jede Vergabe, jede Änderung und jeder Entzug von Rollen und Benutzerberechtigungen muss, unabhängig von der Komponente, dokumentiert und jederzeit nachvollziehbar sein. Es muss immer ein genehmigter Antrag für die Anlage von Benutzern sowie für Vergabe oder den Entzug von Rollen und Berechtigungen vorliegen. Die Anträge sind zu dokumentieren.

3. BENUTZERZUGANGSVERWALTUNG

Der Zugang zu Anwendungen, Betriebssysteme und Datenbanken muss entsprechend der Anforderungen dieser Richtlinie eingeschränkt sein. Hierzu ist je Anwendung, Betriebssystem, Datenbank oder Netzlaufwerk ein Rollen- und Berechtigungskonzept[2] gemäß der Vorlage (siehe 5 Vorlage Rollen- und Berechtigungskonzept) durch den jeweils verantwortlichen Informationseigentümer zu erstellen[3]. Die Rollen- und Berechtigungskonzepte sind mindestens jährlich und bei Änderungen an Anwendungen, Betriebssystemen oder Datenbanken zu überprüfen. Rollen- und Berechtigungskonzept müssen mindestens Angaben zu folgenden Punkten enthalten:

- Name der betroffenen Anwendung / des Betriebssystems / der Datenbank / des Netzlaufwerks,
- Name des Informationseigentümers (Informationssysteme) / des Role-Owners (Netzlaufwerke),
- Festlegung aller Rollen, (fachlich, technisch, administrativ, ggf. nicht benötigt),
- Beschreibung von Sonderrollen (z. B. Revision, Datenschutzbeauftragter etc.),
- Festlegung der Rechte der Rollen (Lesen, Schreiben, Ändern etc.),
- Festlegung der Vergabe-, Entzugs-, Sperr- und Genehmigungsverfahren,
- Berücksichtigung von Funktionstrennungsaspekten, z. B. im Rahmen einer Funktionstrennungsmatrix,
- Erstellung eines Notfalluserkonzepts, soweit erforderlich.

Soweit fachliche oder technische Gründe gegen eine Umsetzung der Vorgaben dieser RIchtlinie sprechen, sind Ausnahmen zwischen dem verantwortlichen Informationseigentümer / Role-Owner und der Stabstelle Datenschutz und Informationssicherheit abzustimmen und zu dokumentieren. Die Rollen- und Berechtigungskonzepte sind durch den jeweiligen Informationseigentümer vorzuhalten und auf Anforderung der Stabstelle Datenschutz und Informationssicherheit vorzulegen.

[2] Clusterungen sind grundsätzlich möglich
[3] Bereits bestehende Rollen- und Berechtigungskonzepte können weiter genutzt werden, soweit diese die hier aufgeführten Anforderungen erfüllen.

3.1. Ablauf und Verantwortlichkeiten

3.1.1. Ablauf

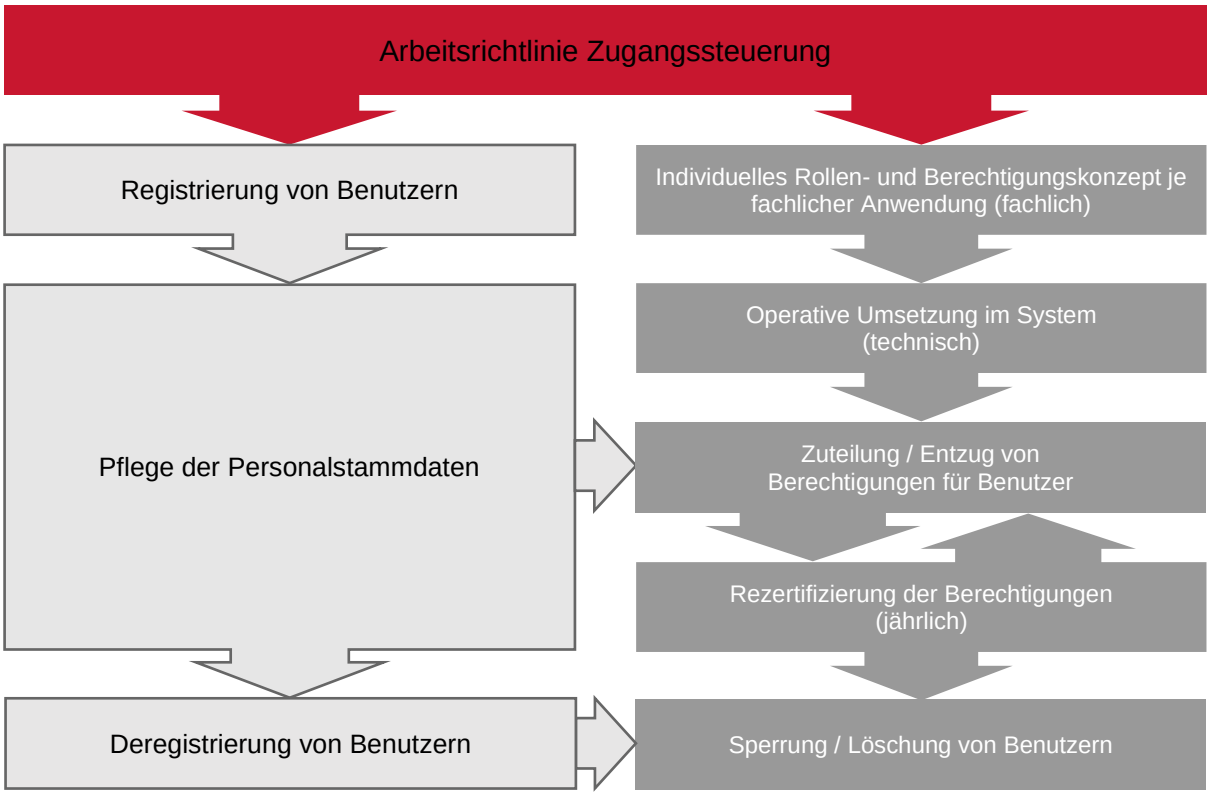

Abbildung 1: Vorgehensweise bei der Zugangssteuerung

3.1.2. Verantwortlichkeiten

AKTION	VERANTWORTLICH	MITWIRKUNG
Registrierung von Benutzern	IT-Support	Abteilung Personal Führungskraft/Auftraggeber (Benutzerzugang)
Pflege der Personalstammdaten	IT-Support	Abteilung Personal Benutzer (Änderung der Personaldaten)
Deregistrierung von Benutzern	IT-Support	Abteilung Personal Führungskraft/Auftraggeber (Benutzerabgang) oder Fristablauf

AKTION	VERANTWORTLICH	MITWIRKUNG
Rollen- und Berechtigungskonzept	Informationseigentümer (Informationssysteme) Role-Owner (Netzlaufwerk)	Produktverantwortlicher
Operative Umsetzung im System (technisch)	IT-Support	Informationseigentümer (Rollen- und Berechtigungskonzept)
Zuteilung/Entzug von Berechtigungen für Benutzer	IT-Support	Führungskraft (Auftrag Zuteilung / Entzug Berechtigungen)
Rezertifizierung der Berechtigungen (jährlich)	Führungskraft und IT/BO	Informationseigentümer (Bericht über Berechtigungen mit Hilfe des IT-Supports)
Sperrung / Löschung von Benutzern	Führungskraft IT-Support	Abteilung Personal (Benutzer Abgang) Stabstelle Datenschutz und Informationssicherheit (Sicherheitsvorfall) Monitoring (Brute-Force-Attacken) Führungskraft (Auftrag Entzug Berechtigungen) Fristablauf

Tabelle 1: Übersicht der Verantwortlichkeiten und Mitwirkungen

3.2. Registrierung, Pflege und Deregistrierung von Benutzern

Bei der Registrierung, Pflege und Deregistrierung von Benutzern sind die nachfolgenden Anforderungen zu berücksichtigen:

- Zu jedem Benutzer ist ein Personalstammdatensatz vorhanden.
- Es ist sicherzustellen, dass die Personalstammdaten der Benutzer immer auf dem aktuellen Stand sind (z. B. Anpassung von Nachnamen oder Familienstand nach Eheschließung).
- Jedes Benutzerkonto muss einer natürlichen Person zugeordnet sein.
- Gemeinsam genutzte Kennungen (insbesondere technische User) sind nur gestattet, wenn dies aus geschäftlichen oder betrieblichen Gründen erforderlich ist.
- Sofortige Deaktivierung von Benutzerkonten im Falle des Ausscheidens von Mitarbeitern. Löschung von Benutzerkonten, ggf. nach Ablauf einer angemessenen Frist.

- Regelmäßige Identifizierung, Löschung oder Deaktivierung nicht mehr benötigter Benutzerkonten.
- Sicherstellung, dass ehemals genutzte Kennungen nicht an andere Benutzer vergeben werden.

3.3. Zuteilung und Entzug von Berechtigungen

Bei der operativen Umsetzung von Berechtigungen müssen folgende Punkte berücksichtigt werden:

- Die Erteilung von Berechtigungen muss grundsätzlich auch befristet möglich sein. Nach Ablauf der Frist muss die jeweilige Berechtigung unverzüglich und möglichst automatisiert entzogen werden.
- Sicherstellung, dass die Zugangsrechte nicht aktiviert, deaktiviert oder gelöscht werden, bevor die Genehmigungsverfahren abgeschlossen sind.
- Anpassung der Zugangsrechte der Benutzer, deren Funktionen oder Tätigkeiten sich geändert haben.Bei rein organisatorischen Veränderungen kann auf eine Anpassung verzichtet werden.

3.4. Verwaltung privilegierter Zugangsrechte

Bei der Zuteilung und der Verwaltung von privilegierten Zugangsrechten
sind nachfolgende Anforderungen zu berücksichtigen:

- Privilegierte Zugangsrechte dürfen Benutzern nur bedarfsgerecht erteilt werden.
- Es muss ein Genehmigungsprozess und eine aktuelle Aufstellung aller gewährten privilegierten Zugangsrechte existieren. Privilegierte Zugangsrechte dürfen nicht vor Abschluss des Genehmigungsprozesses gewährt werden.
- Die bedarfsgerechte Gewährung von privilegierten Zugangsrechten ist mindestens alle 6 Monate zu überprüfen. Dies ist nachvollziehbar zu dokumentieren.
- Privilegierte Zugangsrechte müssen einem anderen als dem Benutzerkonto zugewiesen werden, das für die normalen Geschäftsaktivitäten verwendet wird. Normale Geschäftsaktivitäten dürfen nicht mit dem Benutzerkonto ausgeführt werden, das über privilegierte Zugangsrechte verfügt.
- Privilegierte Zugangsrechte sind eindeutigen Benutzerkonten zuzuweisen, damit Benutzer mit ihren Handlungen in Verbindung gebracht und verantwortlich gemacht werden können.
- Es sind Verfahren zu definieren, einzurichten und anzuwenden, mit denen eine unbefugte Nutzung von Benutzerkonten mit allgemeinen Administratorrechten entsprechend den Konfigurationsmöglichkeiten des Systems verhindert wird.
- Bei Benutzerkonten mit allgemeinen Administratorrechten muss die Vertraulichkeit der geheimen Authentifizierungsdaten bei einer gemeinsamen Nutzung gewahrt werden (z. B. Kennwörter schnellstmöglich nach Ausscheiden oder Versetzung eines Benutzers mit privilegierten Zugangsrechten ändern, Verwendung geeigneter Verfahren zum Mitteilen dieser Kennwörter an Benutzer mit privilegierten Zugangsrechten).

3.5. Überprüfung von Benutzerzugangsrechten

Es ist sicherzustellen, dass in regelmäßigen Abständen (mindestens jährlich) die
Benutzerzugangsrechte durch die jeweilige disziplinarische Führungskraft sowie IT/BO überprüft

werden. Kritische Berechtigungen[4] sind mindestens halbjährlich zu überprüfen. Hierbei ist zu prüfen, ob die Rollen und Berechtigungen den Vorgaben des Berechtigungskonzepts entsprechen. Hierfür sind möglichst technische Prozesse zu etablieren, nebst geeigneten Erinnerungs- und Eskalationsprozessen. Die erfolgte Rezertifizierung ist zu dokumentieren. Notwendige Änderungen sind umgehend zu veranlassen und von der IT umzusetzen.

4. ANFORDERUNGEN AN DIE ZUGANGSSTEUERUNG

4.1. Sichere Anmeldeverfahren

Es ist sicherzustellen, dass der Zugang zu Anwendungen, Betriebssystemen und Datenbanken durch ein sicheres Anmeldeverfahren gesteuert wird.
Der Zugang zu Citrix von außerhalb der VAV ist mit einem zweiten Faktor zu sichern.

4.2. System zur Verwaltung von Kennwörtern

Systeme zur Verwaltung von Kennwörtern sind interaktiv und stellen starke Kennwörter sicher.

4.3. Gebrauch von administrativen Managementwerkzeugen

Der Gebrauch von Hilfs- oder Dienstprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist einzuschränken und streng zu überwachen. Hierzu ist ein formaler Prozess zu definieren, welcher folgende Punkte regelt:

- Verwendung von Identifizierungs-, Authentifizierungs- und Genehmigungsverfahren für Dienstprogramme.
- Trennung der Dienstprogramme von der Anwendungssoftware.
- Beschränkung der Verwendung von Dienstprogrammen auf eine möglichst geringe Zahl vertrauenswürdiger, befugter Benutzer.
- Genehmigung zur Ad-hoc-Verwendung von Dienstprogrammen.
- Beschränkung der Verfügbarkeit von Dienstprogrammen, z. B. für die Dauer einer berechtigten Änderung. Diese Berechtigungen sind mindestens alle 6 Monate zu überprüfen und im Bedarfsfall zu rezertifizieren oder zu entziehen. Dieser Vorgang ist nachvollziehbar zu dokumentieren.
- Festlegung und Dokumentation von Berechtigung für Dienstprogramme.
- Entfernung bzw. Deaktivierung aller nicht notwendiger Dienstprogramme.
- Sperrung von Dienstprogrammen für Benutzer, die Zugang zu Anwendungen auf Systemen haben, bei denen eine Aufgabentrennung erforderlich ist.

4.4. Zugangssteuerung für Quellcode von Programmen

Es ist sicherzustellen, dass der Zugang zu Quellcode von Programmen eingeschränkt ist.

[4] Zu den kritischen Berechtigungen zählen u.a. administrative Berechtigungen. Weiterhin können auch nicht administrative Berechtigungen kritisch sein, wenn z.B. eine Rolle komplette Datensätze löschen kann oder aus fachlicher Sicht mit der Rolle u. U. sensible oder geheimhaltungspflichtige Daten eingesehen werden könnten, also wenn auch fachliche Kritikalität gesehen wird.

5. VORLAGE ROLLEN- UND BERECHTIGUNGSKONZEPT

Die aktuelle Vorlage und Checkliste zur Erstellung eines eigenen Rollen- und Berechtigungskonzept erhalten Sie von der Stabstelle Datenschutz und Informationssicherheit.