Arbeitsrichtlinie Physische und umgebungsbezogene Sicherheit

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Physische und umgebungsbezogene Sicherheit
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	03.12.2020
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
20.0	03.12.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.1.	Daniel Fürdauer
21.0	30.11.2021	Kapitel 3.3.1.: Verallgemeinerung der Brandschutzvorschriften; Kapitel 2.2.3 und 2.2.4.: Klarstellung/Korrektur bei beauftragten Personen	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

Inhaltsverzeichnis 3

1. Einleitung 5

1.1. Zielsetzung 5

1.2. Geltungsbereich 5

1.3. Verantwortlichkeiten 5

2. Allgemeine Anforderungen 6

2.1. Sicherheitszonenkategorien 6

2.2. Sicherheitsmaßnahmen für Sicherheitszonen 7

2.2.1. SZK 0: Unkontrollierter Bereich innerhalb der VAV-Grundstücksgrenzen 7
2.2.2. SZK 1: Überwachter Bereich 7
2.2.3. SZK 2: Vorkontrollierter Bereich 7
2.2.4. SZK 3: Selektiver Bereich 7
2.2.5. SZK 4: Hochsicherheitsbereich 8

2.3. Überwachungsmaßnahmen 8

2.3.1. SZK 0: Unkontrollierter Bereich innerhalb der VAV-Grundstücksgrenzen 8
2.3.2. SZK 1: Überwachter Bereich 8
2.3.3. SZK 2: Vorkontrollierter Bereich 8
2.3.4. SZK 3: Selektiver Bereich 8
2.3.5. SZK 4: Hochsicherheitsbereich 9

3. Gefährdungsabhängige Sicherheitsmaßnahmen 9

3.1. Grundsätzliche Kriterien 9

3.2. Standort 10

3.3. Gebäude 10

3.3.1. Brandschutz, Melde- und Löschtechnik 10
3.3.2. Sicherheitssysteme 10

3.4. Sicherheitsbereiche (Räume, Flächen) 10

3.4.1. Archivräume 10
3.4.2. Technikräume 10
3.4.3. Rechenzentren 11
3.4.4. Öffentliche-, Anlieferungs- und Ladebereiche 11

3.5. Verkabelung 11

3.5.1. Dokumentation 11

3.6. Geräte und Betriebsmittel 12

3.7. Physische Zutrittskontrolle 12

3.7.1. Anforderungen an Zutrittskontrollsysteme 12
3.7.2. Zutrittsschutz 12
3.7.3. Schließsysteme und Schlüsselverwaltung 12

1. EINLEITUNG

1.1. Zielsetzung

Diese Richtlinie dient der Definition und Beschreibung der physischen und umgebungsbezogenen Sicherheitsanforderungen zum Schutz der Unternehmenswerte. Die Sicherheitsanforderungen dienen dazu Verlust, Diebstahl, Beschädigung und anderweitige Gefährdungen von Unternehmenswerten zu verhindern. Dazu gehören neben der Informations- und Kommunikationstechnik und Sachwerten auch die verarbeiteten Daten und sonstigen Informationen.

1.2. Geltungsbereich

Der Geltungsbereich umfasst alle Liegenschaften, Systeme und Services der VAV sowie diejenigen Systeme und Services, die die VAV ggf. für Kunden bereitstellt.

1.3. Verantwortlichkeiten

Das Facility Management ist zuständig für die Gebäudesicherheitsmaßnahmen und deren Überwachung bzw. die Beauftragung und Steuerung deren beauftragten Dienstleister, sowie für die Überwachung berechtigter Zutritte.

2. ALLGEMEINE ANFORDERUNGEN

Die grundsätzliche Philosophie des VAV Gebäudesicherheitskonzepts beschreibt sich wie folgt:

- zutrittskontrolliertes Haus für Mitarbeiter
- offenes Haus für Kunden und Besucher (bis zum Empfang)
- geschlossenes Haus für ungebetene Gäste

2.1. Sicherheitszonenkategorien

Alle Räumlichkeiten und Flächen in der VAV werden Sicherheitszonen zugeordnet. Eine Sicherheitszone ist eine Zusammenfassung von Flächen ähnlichen Schutzbedarfs, die mit entsprechenden Sicherheitsmaßnahmen abzusichern sind. Sicherheitszonen mit ähnlichen Sicherheitsmaßnahmen werden zu einer sogenannten „Sicherheitszonenkategorie“ (SZK) zusammengefasst.
In der VAV werden folgende Sicherheitszonenkategorien verwendet:

SZK	BESCHREIBUNG
SZK 0	Unkontrollierter Bereich Bereiche innerhalb der VAV Grundstücksgrenzen, die für die Öffentlichkeit frei zugänglich sind und keinerlei Überwachung und Zutrittsschutz unterliegen.
SZK 1	Überwachter Bereich VAV Grundstücke, die einer Überwachung und / oder einer ersten Zutrittskontrolle unterliegen.
SZK 2	Vorkontrollierter Bereich Alle Innenbereiche (Büroflächen etc.) der VAV Gebäude, die nur durch Berechtigte (Mitarbeiter, Dienstleister, geladene Besucher) betreten werden dürfen.
SZK 3	Selektiver Bereich Räume mit schützenswerten Inhalten (z. B. Archiv, IT-Bereich, Vorstandsbereich), die nur von einem eingeschränkten Personenkreis betreten werden dürfen.
SZK 4	Hochsicherheitsbereich Räume mit besonders schützenswerten Inhalten (Rechenzentrum), die nur von einem sehr eingeschränkten Personenkreis betreten werden dürfen.

Tabelle 1: Sicherheitszonenkategorien

Für die Identifizierung, Bewertung und Einstufung von Räumlichkeiten und Flächen in diese Sicherheitszonen ist das Facility Management in Abstimmung mit der Stabstelle Datenschutz und Informationssicherheit und Vorstand verantwortlich.
Grundsätzlich ist jede Fläche, die von der VAV genutzt wird, der Sicherheitszonenkategorie 2 (SZK 2) zugeordnet. Die Zuordnung in eine andere Sicherheitszonenkategorie (SZK), beispielsweise aufgrund eines erhöhten Schutzbedarfs, ist durch den jeweiligen Risikoverantwortlichen, Facility Management oder die Stabstelle Datenschutz und Informationssicherheit zu aufzuzeigen.

Am Übergang zwischen zwei unterschiedlichen Sicherheitszonen sind ab der SZK 1 technische, bauliche oder organisatorische Maßnahmen zu etablieren, die es ermöglichen, den Wechsel von Personen und Informationen zwischen den Zonen zu beschränken.

2.2. Sicherheitsmaßnahmen für Sicherheitszonen

2.2.1. SZK 0: Unkontrollierter Bereich innerhalb der VAV-Grundstücksgrenzen

Der Übergang aus öffentlichen Bereichen in die SZK 0 wird nicht aktiv beschränkt. Die VAV besitzt in dieser Sicherheitszone jedoch ein Hausrecht und darf Personen auffordern, das Grundstück zu verlassen oder kann die Nutzung des Grundstücks einschränken.
Zulässige Maßnahmen sind z. B. Platzverweise oder Schilder, auf denen die Nutzung des Grundstücks geregelt wird.

2.2.2. SZK 1: Überwachter Bereich

Der Zutritt von Personen und die Zufahrt von Fahrzeugen in die SZK 1 muss aktiv überwacht werden oder mittels einer baulichen Sicherheitsmaßnahme versehen sein.
Die Funktionsfähigkeit von Sicherheitsmaßnahmen (z. B. Sicherheitstüren, Zustand von Zäunen, Sichtbeschränkung durch Pflanzenwuchs) ist in angemessenen Zeiträumen zu kontrollieren. Werden Mängel festgestellt, sind diese umgehend zu beseitigen.

2.2.3. SZK 2: Vorkontrollierter Bereich

Die Identität aller Personen in der SZK 2 muss bekannt sein. Hierzu ist beim Zutritt in die Sicherheitszone die Identität von Personen festzustellen.
Das Umgehen der Schutzfunktion ist durch personelle, organisatorische oder bauliche Sicherheitsmaßnahmen zu verhindern.
Betriebsfremde Personen dürfen sich innerhalb der SZK 2 nur in Begleitung eines Mitarbeiters bewegen. Hiervon ausgenommen sind Personen, die im Rahmen einer Beauftragung Aufgaben in der SZK 2 auf dem Gelände der VAV durchführen müssen und Personen, die zu diesem Zweck auch einen Zutritts-Chip erhalten haben und denen entsprechende Berechtigungsrollen zugewiesen wurden.
Der Zutritt mit dem Zutrittskontrollsystem ist zu protokollieren bzw. zu dokumentieren.

2.2.4. SZK 3: Selektiver Bereich

Der dauerhafte Zutritt zu Sicherheitszonen der SZK 3 darf nur Personen gewährt werden, für die ein fachlicher Bedarf identifiziert und eine entsprechende Berechtigungsrolle zugewiesen wurde.
Am Übergang in die SZK 3 ist die Identität der Person zu prüfen.
Betriebsfremde Personen dürfen in Sicherheitsbereiche der SZK 3 nur in Begleitung eines internen verantwortlichen Mitarbeiters mitgenommen werden. Hiervon ausgenommen sind Personen, die im Rahmen einer Beauftragung Aufgaben in der SZK 3 auf dem Gelände der VAV durchführen müssen und Personen, die zu diesem Zweck auch einen Zutritts-Chip erhalten haben und denen entsprechende Berechtigungsrollen zugewiesen wurden.

Begleiter haben mitgenommene Personen durchgängig zu beaufsichtigen. Nach Ende der Tätigkeit ist diese Person aus dem Bereich hinaus zu begleiten.
Zutritte sind zu dokumentieren bzw. zu protokollieren.

2.2.5. SZK 4: Hochsicherheitsbereich

Zusätzlich zu den Anforderungen der SZK 3 dürfen in der SZK 4 nur Personen Zutritt erhalten, denen die Berechtigung explizit erteilt wurde.
Das Mitnehmen einer anderen Person ist nur in Begleitung einer berechtigten Person möglich.
Das Umgehen des Zutrittskontrollsystems ist durch geeignete organisatorische Maßnahmen zu verhindern.
Potenzielle Schwachstellen im Zutrittskontrollsystem müssen durch eine zusätzliche Überwachungsmaßnahme, wie z. B. eine Alarmanlage und eine Videoüberwachung, kompensiert werden.

2.3. Überwachungsmaßnahmen

Innerhalb der Sicherheitszonen sind folgende Überwachungsmaßnahmen durch alle VAV Mitarbeiter vorzusehen:

2.3.1. SZK 0: Unkontrollierter Bereich innerhalb der VAV-Grundstücksgrenzen

Regelmäßige Begehungen mit dem Ziel, das Eigentum der VAV zu schützen und Gefahrenquellen für Personen zu beseitigen.

2.3.2. SZK 1: Überwachter Bereich

Aktives Ansprechen von Personen, die sich in diesem Bereich längere Zeit unbegründet aufhalten, sich verdächtig verhalten oder offensichtlich Informationen über die Absicherung der Liegenschaften sammeln.

2.3.3. SZK 2: Vorkontrollierter Bereich

- Organisatorische Anweisung für alle Mitarbeiter, wie mit Personen ohne Berechtigung zu verfahren ist.
- Regelmäßige Überprüfung der Zutrittskontrollsysteme auf Beschädigung und Funktion.

2.3.4. SZK 3: Selektiver Bereich

- Organisatorische Anweisung für alle Mitarbeiter, wie mit Personen ohne Berechtigung zu verfahren ist.
- Regelmäßige Überprüfung der Sicherheitsmaßnahmen zwischen den Sicherheitsbereichen auf Beschädigung und Funktion.

2.3.5. SZK 4: Hochsicherheitsbereich

- Organisatorische Anweisung für alle Mitarbeiter, wie mit Personen ohne Berechtigung zu verfahren ist.
- Die Videotechnik muss im Rahmen der kontinuierlichen Verbesserung dem Stand der Technik angepasst werden.

3. GEFÄHRDUNGSABHÄNGIGE SICHERHEITSMAßNAHMEN

Unabhängig von den oben genannten Sicherheitsmaßnahmen für die definierten Sicherheitszonen, sind Maßnahmen zur Vermeidung von äußeren Einflüssen oder menschlichem Einwirken zu ergreifen. Der Bereich der physischen Informationssicherheit beginnt mit einfachen Mitteln wie verschlossenen Systemgehäusen und reicht bis zum Einschließen von Systemen in Rechenzentren. Alle physischen Sicherheitsanforderungen zielen auf eine Abschottung der Systeme vor Gefahrenquellen hin, wie:

- Mechanische Einwirkungen durch Personen
- Höhere Gewalt (z. B. Wassereinbruch, Brand)
- Einbringung von Schadstoffen (z. B. Staub, Aerosole)
- Elektromagnetische Einwirkung (z. B. Blitzschlag, Überspannung)
- Gasförmige, korrosive Luftbelastungen

3.1. Grundsätzliche Kriterien

In Bezug auf die physische und umgebungsbezogene Sicherheit gibt es grundsätzliche Kriterien, die für die Sicherheitsanforderungen von Belang sind. Die nachfolgenden Kriterien an die physische und umgebungsbezogene Sicherheit sind entlang des Lebenszyklus von

- der Planung und Konzeption,
- der Umsetzung, dem Aufbau und der Inbetriebnahme,
- dem Betrieb,
- bis zur Aussonderung bzw. Außerbetriebnahme zu beachten.

Insbesondere ist bereits bei der Planung und Konzeption von Standorten, Gebäuden, Räumen und Verkabelungen auf eine zukunftssichere, bedarfsgerechte und wirtschaftliche Ausführung unter Beachtung der physischen und umgebungsbezogenen Sicherheit zu achten. Folgende Sicherheitsanforderungen gilt es dabei zu berücksichtigen:
Sicherheitsanforderungen an

- das Umfeld,
- die Baukonstruktion,
- Brandschutz, Melde- und Löschtechnik,
- Sicherheitssysteme und die Sicherheitsorganisation,
- die Energieversorgung und Überspannungsschutz,
- Raumlufttechnische Anlagen und
- die Organisation und Dokumentation.

3.2. Standort

Bereits bei der Planung und Auswahl eines geeigneten Standorts von Gebäuden für Büroflächen, IT-Betrieb und insbesondere für Rechenzentren, müssen standortabhängige Gefährdungen analysiert und berücksichtigt werden.

3.3. Gebäude

Die geplante Nutzung eines Gebäudes und der Schutzbedarf der dort betriebenen Geschäftsprozesse bestimmt, wie ein Gebäude zu gestalten und unter Sicherheitsaspekten auszustatten ist.

3.3.1. Brandschutz, Melde- und Löschtechnik

Der Brandschutz muss den jeweils gültigen Brandschutzvorschriften entsprechen.

3.3.2. Sicherheitssysteme

Für einen Schutz vor vorsätzlichen Handlungen müssen Sicherheitssysteme installiert werden. Hierzu zählt z. B. die Einbruchmeldeanlage, um Diebstahl (Hardware wie Daten), Sabotage und Vandalismus frühzeitig zu entdecken, Akteure abzuschrecken und rechtzeitig Gegenmaßnahmen einzuleiten.
Der Einbruchschutz ist mehrstufig auszulegen. Ab SZK 2 ist zu bewerten, ob diese mittels einer Einbruchmeldeanlage überwacht werden müssen.
Alle physisch mechanischen Maßnahmen (Barrieren) und die überwachenden Sicherheitstechniken im Rahmen des Perimeterschutzes sind durch adäquate personelle / organisatorische Maßnahmen zu ergänzen.

3.4. Sicherheitsbereiche (Räume, Flächen)

Pläne zu Sicherheitszonen sind als vertrauliche Dokumente zu klassifizieren und sicher zu verwahren.
Facility Management bewertet insbesondere unter Beachtung der jeweiligen technischen Möglichkeiten, des jeweiligen Bedarfs und der jeweiligen Sicherheitsanforderungen, ob zentrale IT-/TK-Systeme und versorgungstechnische Systeme und Komponenten im Sicherheitsbereich von Technikräumen zu betreiben sind.

3.4.1. Archivräume

Wasserführende Leitungen in und an Archivräumen sind weitestgehend zu vermeiden.
Fenster und Türen sind geschlossen zu halten.
Die sichere Funktionsweise von Tür- und Fensterverschlüssen und die Einhaltung auf das Verschließen der Türen und Fenster durch die berechtigten Mitarbeiter ist regelmäßig zu überprüfen.

3.4.2. Technikräume

Für Technikräume gelten mindestens die Sicherheitsanforderungen wie für Archivräume. Zusätzlich sind nachfolgende Sicherheitsanforderungen zu berücksichtigen:

Die Absicherung und Auslegung der Stromkreise müssen den tatsächlichen Bedürfnissen angepasst sein.
Bei Anforderungen an die Systemverfügbarkeit durch Redundanz ist darauf zu achten, diese durch unabhängig voneinander führende Versorgungsstränge anzubinden bzw. diese bereitzustellen.
IT-/TK- und Supportsysteme sind mit Überspannungsschutz sowie entsprechend der Verfügbarkeitsanforderungen mit einer USV auszustatten.
Bei Notfällen ist primär die Unversehrtheit der darin tätigen Personen sicherzustellen.

3.4.3. Rechenzentren

Für Rechenzentren gelten mindestens die Sicherheitsanforderungen wie für Technikräume. Zusätzlich sind nachfolgende Sicherheitsanforderungen zu berücksichtigen:
Es sind nach Möglichkeit einbruchshemmende Maßnahmen wie Rollläden, Brandschutztüren, Ziegelwände und dergleichen umzusetzen.

3.4.4. Öffentliche-, Anlieferungs- und Ladebereiche

Produktive IT- und Kommunikationskomponenten dürfen nicht in öffentlich zugänglichen oder in Anlieferungs- und Ladebereichen unbeaufsichtigt oder ohne besondere Schutzvorkehrungen betrieben oder gelagert werden.
An den Übergängen zu anderen Sicherheitszonen sind die jeweiligen Sicherheitsanforderungen zu beachten. So darf es nicht möglich sein, von Anlieferungs- und Ladebereichen unautorisiert in andere Gebäudeteile zu gelangen bzw. unbefugt von außen hierher einzudringen.

3.5. Verkabelung

Bei der Auswahl von Kabeln und Verteilern sind neben der übertragungstechnischen Notwendigkeit und Art der Übertragung, Typ und Topologie, die vorgesehenen Trassensysteme sowie die Umgebungsbedingungen, bei der Verlegung sowie im Betrieb, zu berücksichtigen.

Bei der Planung, Konzeption und Verlegung und Änderung/Rückbau von Strom-, IT- und TK-Verkabelungen sind die entsprechenden einschlägigen Normen sowie die Herstellvorgaben zu beachten, insbesondere Vorschriften zur strukturierten Verkabelung und zum Brandschutz.
Kabelleitungen, -trassen und -verteiler sind in allen Bereichen so zu planen und zu erstellen, dass diese im Betrieb bspw. vor unbefugten Zugriffen, höherer Gewalt sowie Feuer- und Sabotagerisiken geschützt sind.

3.5.1. Dokumentation

Eine entsprechend ausreichende Dokumentation ist mit allen notwendigen Informationen zur Verkabelung ist vorzuhalten.
Verkabelungen sind nach Abschluss der Installation einem festgelegten Abnahmeprozess zu unterziehen, der auch die Aspekte der IT-Sicherheit umfasst.

Geplante und konzeptionierte Verkabelungen sind geeignet und ausreichend zu dokumentieren sowie zu aktualisieren. Die Dokumentation der Verkabelung ist sicher aufzubewahren und der Zugriff entsprechend zu regeln.
Für die Verteilerräume sind Dokumentationen vorzuhalten, die den aktuellen Stand von Rangierungen und Leitungsbelegungen, möglichst neutral (z.B. kein Hinweis auf Nutzungsart), wiedergeben. Nur bestehende und genutzte Verbindungen sind darin aufzuführen.

3.6. Geräte und Betriebsmittel

Geräte und Betriebsmittel sind vor Verlust, Beschädigung, Diebstahl und Unterbrechungen der Betriebstätigkeit zu schützen.
Betriebsmittel sind entsprechend der empfohlenen Herstellervorgaben und Spezifikationen sowie der vorliegenden Einsatzbedingungen zu warten.
Unterstützende Versorgungseinheiten (z. B. USV, Klimaanlage) müssen regelmäßig durch geeignetes Fachpersonal gewartet werden.
Reparaturen und Wartungsarbeiten sind ausschließlich von autorisierten Mitarbeitern oder Servicepartnern durchzuführen.
Alle Fehler sowie alle Instandhaltungs- und Reparaturmaßnahmen sind nachvollziehbar zu dokumentieren.
Für die Wartung von Betriebsmitteln sind geeignete Maßnahmen umzusetzen, unter Berücksichtigung, ob die Wartung von Mitarbeitern vor Ort oder von externen Dritten durchgeführt wird.
Vor Wiederinbetriebnahme von Betriebsmitteln sind diese zu untersuchen, um sicherzustellen, dass diese nicht manipuliert wurden und keine Fehlfunktionen aufweisen.

3.7. Physische Zutrittskontrolle

3.7.1. Anforderungen an Zutrittskontrollsysteme

Für eine wirkungsvolle Zutrittskontrolle müssen Zutrittskontrollsysteme aus mechanischen, elektrischen bzw. elektronischen Komponenten bestehen. Diese Komponenten müssen hinsichtlich ihrer Sicherheitsleistung aufeinander abgestimmt sein.
Die Nutzung von Zutrittskontrollsystemen ist ausreichend zu dokumentieren und mit dem Datenschutzbeauftragten abzustimmen.

3.7.2. Zutrittsschutz

Externes Reinigungs-/Wartungspersonal ist vor dem Einsatz durch den Dienstleister zu überprüfen.
Die Bestimmungen für den Zutritt und die Erbringung der Dienstleistungen in den verschiedenen Sicherheitsbereichen sind schriftlich zu regeln.

3.7.3. Schließsysteme und Schlüsselverwaltung

Für alle mechanischen und elektronischen Schlüssel eines Gebäudes (von Etagen, Fluren und Räumen) muss ein aktueller Schließplan vorhanden sein.

Eine Schlüsselverwaltung ist einzurichten. Diese beinhaltet die Schlüsselgenerierung bei elektronischen Schließsystemen, die Definition von Schließgruppen, die sichere Verwahrung nicht ausgegebener Schlüssel und Reserveschlüssel, die Kontrolle über auszugebende Schlüssel durch Quittierung sowie Sofortmaßnahmen bei Diebstahl und Verlust.
Bei Zuständigkeitsänderungen (und Ausscheiden) von Mitarbeitern sind deren Schließberechtigungen zu prüfen und Schlüssel ggf. einzuziehen.
Schließsysteme sind in regelmäßigen Abständen auf mögliche Sicherheitslücken zu überprüfen (z. B. Sicherheitslücken in RFID-basierenden Systemen).