

Arbeitsrichtlinie Clean Desk

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern

Version 21.0

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Clean Desk
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	10.10.2019
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	10.10.2019	Erstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Redaktionelle Änderungen und Spezifizierung des Umgangs mit Informationen in Besprechungsräumen (Seite 5)	Daniel Fürdauer
21.0	08.11.2021	Redaktionelle Änderung/Klarstellung in Kapitel 1	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	4
2. Rollen und Verantwortlichkeiten	4
2.1. Mitarbeiter	4
2.2. Führungskräfte	4
3. Vorgaben	5

1. ZIELSETZUNG

Mit der nachfolgenden Clean Desk-Strategie soll sichergestellt werden, dass vertrauliche und streng vertrauliche Informationen sicher am Arbeitsplatz (in den Räumlichkeiten der VAV, unterwegs und im Homeoffice) verwahrt werden. Ziel ist es dabei, Zugriffe von unautorisierten Dritten zu verhindern und sicherzustellen, dass die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen nicht negativ beeinflusst wird. Informationen können dabei auf Papier vorliegen (Schriftstücke, Ausdrücke etc.). Des Weiteren können Informationen auf Datenträgern (z.B. USB-Sticks, Festplatten) oder mobilen Endgeräten (z.B. Smartphones) gespeichert sein oder aber in Form von Präsentationen zugänglich gemacht werden. Die Richtlinie umfasst dabei alle vorgenannten Speicher- und Ablageformen.

2. ROLLEN UND VERANTWORTLICHKEITEN

2.1. Mitarbeiter

Jeder Mitarbeiter ist zur Umsetzung der unter Punkt 3 genannten Vorgaben der Clean Desk-Strategie verpflichtet.

2.2. Führungskräfte

Die Führungskräfte sind dafür verantwortlich, stichprobenartig in ihrem Bereich die Umsetzung der Clean Desk-Strategie zu überprüfen und die Mitarbeiter bei Abweichungen auf ein „korrektes Aufräumen“ im Sinne dieser Arbeitsrichtlinie hinzuweisen.

3. VORGABEN

- Jeder Mitarbeiter hat dafür Sorge zu tragen, dass er seinen Arbeitsplatz ordentlich und sauber hinterlässt. Ordnung und Sauberkeit am Arbeitsplatz sind wichtige Elemente der Sicherheit.
- IT-Benutzer haben darauf hinzuwirken, dass Unbefugte keinen Zugang zu IT-Anwendungen oder Zugriff auf Daten erhalten.
- Für die momentane Arbeit nicht benötigte Informationen sind sicher unterzubringen, hierzu zählen klassifizierte Dokumente ebenso wie Notizen oder Mitschriften.
- Insbesondere sind vertraulich und streng vertraulich klassifizierte Informationen unter Verschluss zu halten, wenn sie nicht unter Aufsicht stehen.
- In öffentlichen Bereichen sind auch interne Dokumente gegen den Zugriff externer Personen zu sichern.
- Datenträger (z.B. USB-Sticks, Festplatten) sind insbesondere aufgrund einer Virengefahr unter Aufsicht bzw. unter Verschluss zu halten, unabhängig von der Klassifizierung der gespeicherten Informationen.
- Nicht-stationäre Arbeitsmittel (Laptops, mobile Endgeräte etc.) sind sicher zu verwahren.
- Ausdrücke mit vertraulichem oder streng vertraulichem Inhalt dürfen nicht unbeaufsichtigt im oder am Drucker verbleiben.
- Bei temporärer Abwesenheit vom Arbeitsplatz ist der Arbeitsplatzrechner zu sperren. Bei Arbeitsende ist der Arbeitsplatzrechner grundsätzlich vollständig herunterzufahren.
- Für alle Arbeitsplätze sind automatische Bildschirmsperren einzurichten, die sich nach 10 Minuten einschalten.
- Sind längere Abwesenheiten geplant (Urlaub, Dienstreisen, Fortbildungen etc.), ist der Arbeitsplatz so aufzuräumen, dass keine internen, vertraulichen oder streng vertraulichen Informationen am Arbeitsplatz zurückgelassen werden. Bei längeren Abwesenheiten während der Arbeitszeit und bei Arbeitsende sind alle vertraulichen und streng vertraulichen Informationen sicher zu verschließen, z.B. in Schränken oder Rollcontainern.
- Sind Dokumente oder Datenträger zu entsorgen, so hat dies entsprechend der Arbeitsrichtlinie „Entsorgung von Datenträgern“ zu geschehen.
- Bei Informationen auf digitalen Anzeigegeräten wie beispielsweise Monitoren oder Mobile Devices, ist darauf zu achten, dass diese Informationen nur durch berechtigte Personen eingesehen werden können.
- Handouts sind nach der Besprechung einzusammeln, ggf. benutzte Flipcharts oder andere Hilfsmittel sind zu entfernen. Eine Abmeldung von den Thin Clients / Desktop PC ist obligatorisch.
- Werden in Besprechungsräumen als intern, vertraulich oder streng vertrauliche Informationen präsentiert, so ist dafür Sorge zu tragen, dass diese Informationen nicht von außen (durch Fenster und Türen) durch Unbefugte einsehbar sind und nicht im Besprechungsraum verbleiben.
- Passwörter dürfen auf keinen Fall sichtbar (am Monitor, in der unverschlossenen Schublade, unter der Schreibtischunterlage etc.) verwahrt werden.