Arbeitsrichtlinie Telearbeit

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Telearbeit
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	02.03.2020
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	02.03.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
21.0	09.11.2021	Redaktionelle Änderungen in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.1.	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. EINLEITUNG

Unter Telearbeit wird jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ausschließlich oder zeitweise außerhalb der Geschäftsräume und Gebäude des Arbeitgebers verrichtet wird. Die Erledigung der Tätigkeiten wird durch eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers unterstützt. Um Sicherheitsrisiken zu minimieren, müssen insbesondere Vorkehrungen zur Absicherung der Kommunikation sowie zur Identifizierung- und Authentisierung der Nutzer getroffen werden.

2. ABGRENZUNG

Telearbeit ist der Oberbegriff und enthält alle Varianten, bei denen berechtigte Mitarbeiter und externe Personen Arbeiten von zu Hause oder einem anderen Ort aus verrichten, indem sie mit einem elektronischen Kommunikationsnetz mit der VAV verbunden ist. Hierbei werden folgende Formen in der VAV unterschieden:

1. **Teleheimarbeit (auch Homeoffice genannt):** Hier verrichtet der Mitarbeiter die gesamte Arbeit außerhalb der Räumlichkeiten der VAV. Ein Arbeitsplatz in den Räumlichkeiten der VAV existiert nicht.
2. **Alternierende Telearbeit:** Hierbei wird sowohl von zu Hause als auch in der VAV gearbeitet.
3. **Mobile Telearbeit (auch Remote-Arbeit genannt):** Hierbei stehen die Tätigkeit an wechselnden Arbeitsorten oder von unterwegs sowie der Fernzugriff auf die VAV-Infrastruktur im Mittelpunkt.

Diese Arbeitsrichtlinie gilt für alle Varianten und gilt auch explizit für die Zulassungsstellen und regelt die entsprechenden Anforderungen für die Zulassungsstellen.

3. ALLGEMEINE ANFORDERUNGEN

Für alle Varianten sind insbesondere folgende Informationssicherheits- und datenschutzrelevante Aspekte zu beachten.

3.1. Schutz von Informationen gegen Zugriffe und Kenntnisnahme Dritter

Informationen in digitaler und in Papierform müssen gegen unberechtigte Zugriffe geschützt werden. Hierzu zählt auch der physische Zugriff auf IT-Systeme, Diensttelefone und sonstige dienstlich zur Verfügung gestellte Hardware. Die Vorgaben hierzu sind der Arbeitsrichtlinie Clean Desk zu entnehmen.
Papierdokumente sind, je nach Kritikalität, entsprechend zu entsorgen. Intern, vertraulich und streng vertraulich eingestufte Dokumente dürfen nur in geeigneten Containern der VAV oder in entsprechenden Datenvernichtern (Aktenvernichter) entsorgt werden. Mobile Datenträger sind immer über die VAV zu entsorgen.
Der Bildschirm ist so zu platzieren, dass die Kenntnisnahme des Bildschirminhaltes durch Dritte verhindert wird. Ebenso ist der Bildschirm zu sperren, wenn der Arbeitsplatz verlassen wird. Es sind technische Maßnahmen zu etablieren, die den Bildschirm nach einer gewissen Dauer der Inaktivität automatisch sperren. Die Aufhebung der Sperrung darf nur durch erneute Authentifikation erfolgen.

Die Anbindung an das lokale Netz muss nach einem gängigen Verfahren Ende-zu-Ende verschlüsselt werden. Die Anforderung an die kryptografischen Schlüssel sind der Arbeitsrichtlinie Kryptographie zu entnehmen.
Interne und (streng) vertrauliche Daten auf digitalen Datenträgern dürfen nur verschlüsselt transportiert werden.

3.2. Physische Sicherheit des Arbeitsorts

Der Arbeitsort ist so zu wählen und einzurichten, dass die Vertraulichkeit und Verfügbarkeit der Tätigkeit zu jedem Zeitpunkt sichergestellt ist.

3.3. Datenablage

Die Speicherung von Daten darf technisch nur auf den durch Berechtigungen erteilten Speicherorten erfolgen. Eine lokale Speicherung ist zu unterbinden. Dies gilt sowohl für die Zwischenablage als auch für Druckausgaben. Falls keine Verbindung zum Zeitpunkt der Speicherung in das VAV Netzwerk besteht, darf ausnahmsweise lokal zwischengespeichert werden. Anschließend ist sicherzustellen, dass die lokale Kopie an den freigegebenen Speicherort verschoben wird.

3.4. Heim- und Fremdnetzwerke

Es muss sichergestellt sein, dass keine Dateien aus dem VAV Netzwerk in das Heim-/Fremdnetzwerk und umgekehrt kopiert werden können.

3.5. Schutz vor Umwelteinflüssen

Die Betriebsmittel sind angemessen gegen Schäden, wie z. B. Überspannung und Feuchtigkeit zu schützen.

3.6. Datenschutz

Die Telearbeiter sind auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen. Die bestehenden Datenschutzanforderungen gelten auch bei der Telearbeit. Regelungen hierzu sind in der Konzernrichtlinie Datenschutz beschrieben.

3.7. Regelungen / Vereinbarungen

Alle relevanten Aspekte der Telearbeit müssen vertraglich oder durch eine Betriebsvereinbarung geregelt werden. Zu Informationszwecken sind Telearbeitern die geltenden Regelungen oder ein dafür vorgesehenes Merkblatt auszuhändigen, das die zu beachtenden Sicherheitsmaßnahmen erläutert.

3.8. Meldewege

Datenschutz und sicherheitsrelevante Vorfälle sind entsprechend der Vorgaben im Intranet im Datenschutz-und Informationssicherheits-Bereich (Richtlinie Data Breach Prozess bzw. Arbeitsrichtlinie Sicherheitsvorfall) zu melden.

4. SPEZIELLE ANFORDERUNGEN

4.1. Telearbeitsplatzrechner

4.1.1. Sicherheit des Telearbeitsrechners

Telearbeitsplatzrechner müssen die gleichen Anforderungen erfüllen wie die in der VAV genutzten Rechner.
Es muss sichergestellt werden, dass nur autorisierte Personen auf die Telearbeitsrechner zugreifen können. Darüber hinaus muss der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

4.1.2. Anbindung an die VAV

Die Anbindung des Arbeitsplatzes erfolgt mittels einer verschlüsselten Verbindung durch Citrix über das Internet.
Die Möglichkeit zum Übertragen von Daten aus der Citrix-Umgebung auf den Telearbeitsrechner wird unterbunden.
Bei der Authentifizierung ist ein zweiter Faktor zu nutzen.

4.1.3. Wartung und Support

Die von der VAV zu dienstlichen Zwecken zur Verfügung gestellten Arbeitsmittel (z. B. PC / Notebook/ Thin Client, Telefon, Router) sind durch die IT fernzuwarten. Dies schließt auch die Installation von Sicherheitspatches und aktuellen Virenschutzsignaturen mit ein.

4.2. Virtueller Desktop

4.2.1. Virtueller Desktop

Als Arbeitsoberfläche ist ein virtueller Desktop zur Verfügung zu stellen, auf dem nur die für die Tätigkeit benötigten Applikationen, Server- und Diensteverbindungen zur Verfügung stehen. Eine lokale Speicherung von Daten, die Nutzung der Zwischenablage und der lokale Druck sind technisch zu unterbinden.

4.2.2. Sicherheit des Telearbeitsrechners

Telearbeitsplatzrechner müssen über eine stets aktuelle Internet Security (Virenschutz, Firewall, etc.) verfügen und stets die aktuellen Sicherheitspatches installiert haben.

Es muss sichergestellt werden, dass nur autorisierte Personen auf den Virtuellen Desktop zugreifen können.

4.2.3. Anbindung an die VAV

Die Anbindung des Arbeitsplatzes erfolgt mittels einer verschlüsselten Verbindung durch Citrix über das Internet.
Die Möglichkeit zum Übertragen von Daten aus der Citrix-Umgebung auf den Telearbeitsrechner wird unterbunden.
Bei der Authentifizierung ist ein zweiter Faktor zu nutzen.

4.2.4. Wartung und Support

Der Mitarbeiter wartet die eigenen Arbeitsmittel (z. B. PC / Notebook, Router) selbst, dies schließt auch die Installation von Sicherheitspatches und aktuellen Virenschutzsignaturen mit ein.
Die IT der VAV kann den Mitarbeiter bei Bedarf zum Beispiel mittels Fernwartung dabei unterstützen.

4.3. VPN Zugang

4.3.1. Sicherheit des Telearbeitsrechners

Telearbeitsplatzrechner müssen die gleichen Anforderungen erfüllen wie die in der VAV genutzten Rechner.
Es muss sichergestellt werden, dass nur autorisierte Personen auf die Telearbeitsrechner zugreifen können. Darüber hinaus muss der Telearbeitsrechner so abgesichert werden, dass er nur für autorisierte Zwecke benutzt werden kann.

4.3.2. Zugang

Der Zugang zum VAV Netz muss über ein VPN erfolgen und über einen zweiten Faktor zusätzlich abgesichert werden. Die Verschlüsselung richtet sich nach den Vorgaben der Arbeitsrichtlinie Kryptographie. Die Verbindung ist nach einer angemessenen Zeit der Inaktivität zu terminieren.

4.3.3. Wartung und Support

Die von der VAV zu dienstlichen Zwecken zur Verfügung gestellten Arbeitsmittel (z. B. PC / Notebook/ Thin Client, Telefon, Router) sind durch die IT fernzuwarten. Dies schließt auch die Installation von Sicherheitspatches mit ein.