Arbeitsrichtlinie Personalsicherheit

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Personalsicherheit
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	12.02.2020
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	12.02.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
21.0	09.11.2021	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. EINLEITUNG

Zur Gewährleistung der Informationssicherheit ist es erforderlich, dass sich alle Mitarbeiter ihrer Verantwortlichkeiten bewusst sind. Ferner müssen sie zur Ausübung der ihnen übertragenen Aufgaben geeignet sein. Um dies zu gewährleisten, ist es erforderlich, dass Sicherheitsaspekte in den verschiedenen Phasen des Beschäftigungsverhältnisses angemessen berücksichtigt werden. Welche Anforderungen vor, während und nach Ablauf eines Beschäftigungsverhältnisses bestehen, ist nachfolgend beschrieben.

2. ROLLEN UND VERANTWORTLICHKEITEN

2.1. Geschäftsleitung

Die Geschäftsleitung trägt die Verantwortung dafür, eine Sicherheitspolitik für das Unternehmen zu erlassen und die Sicherheitsgrundsätze festzulegen. Ferner ist die Geschäftsleitung dafür verantwortlich, eine angemessene Personal- und Kostenausstattung entsprechend des Risikoprofils des Unternehmens sicherzustellen.

2.2. Personalabteilung

Die Personalabteilung ist dafür verantwortlich,

- einen geeigneten Bewerbungs- und Auswahlprozess entsprechend der gesetzlichen Vorgaben zu etablieren,
- die notwendigen Verpflichtungserklärungen (z. B. zum Datenschutz und zur Vertraulichkeit) einzuholen und sicher zu verwahren,
- Qualifikationsnachweise (Zeugnisse etc.) einzuholen und zu prüfen,
- weitere Nachweise (z. B. Führungszeugnisse) unter Beachtung der gesetzlichen Vorschriften anzufordern und zu überprüfen,
- die Zuverlässigkeit / Vertrauenswürdigkeit des Bewerbers zu beurteilen,
- die Sperrung des Mitarbeiters nach Austritt in den Personalsystemen zu veranlassen.

Ferner legt die Personalabteilung in Abstimmung mit der Geschäftsleitung fest, welche Dokumente von Bewerbern verpflichtend einzureichen sind und wie die Prüfung der Dokumente zu erfolgen hat. Darüber hinaus legt die Personalabteilung die Vertragsbedingungen in Abstimmung mit den Fachbereichen fest und veranlasst die Vertragsunterzeichnungen. Zudem muss die Personalabteilung sicherstellen, dass die Arbeitsvertragsunterlagen sicher in der Personalabteilung verwahrt und vertraulich behandelt werden.

2.3. Mitarbeiter

Mitarbeiter im Sinne dieser Richtlinie sind Bewerber, Angestellte, Leiharbeitnehmer, Auszubildende, Praktikanten und Aushilfen. Die Mitarbeiter sind dafür verantwortlich, die für sie relevanten Richtlinien und Anweisungen zu beachten.

2.4. Führungskraft

Die Führungskräfte haben die Aufgabe, folgendes sicherzustellen:

- Beschreibung der Stellenausschreibung (Festlegung der fachlichen und persönlichen Eignungskriterien) und Abstimmung mit der Personalabteilung.
- Prüfung der fachlichen Eignung von Mitarbeitern
- Treffen der Auswahlentscheidungen im Auswahlprozess
- Einweisung der Mitarbeiter in die für den Aufgabenbereich relevanten Richtlinien / Anweisungen
- Sensibilisierung für den Datenschutz und die Informationssicherheit
- Hinweis auf verpflichtende Schulungen (z.B. nach IDD) und Verantwortung für die zeitgerechte Absolvierung dieser durch die eigenen Mitarbeiter
- Erstellung der Funktionsbeschreibungen für die eigenen Mitarbeiter, Abstimmung der Funktionsbeschreibung mit der Personalabteilung (Ablage erfolgt in der Personalabteilung)
- Sicherstellung von angemessenen Vertretungsregelungen,
- Erstellung von Zeichnungsrichtlinien / Vollmachten,
- Gewährleistung, dass Unternehmenseigentum (Mobile Endgeräte, Speichermedien etc.) nach Beendigung des Arbeitsverhältnisses oder bei Änderung der Tätigkeit eingezogen werden.
- Sicherstellung, dass Berechtigungen entzogen werden.
- Löschung der Mitarbeiter Accounts und Laufwerke nach Ablauf der vorgesehenen Fristen.

3. VOR DER BESCHÄFTIGUNG

3.1. Einstellungsprüfungen

Alle Personen, die sich um ein Beschäftigungsverhältnis bewerben, müssen vor der Einstellung einer Überprüfung durch die Personalabteilung unterzogen werden, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen sowie in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen und etwaigen Risiken, die mit der vorgesehenen Aufgabe einhergehen, stehen.
Zur Überprüfung der Sicherheit des Bewerbers sind folgende Informationen – unter Berücksichtigung der jeweils geltenden Gesetze und der jeweiligen Anforderungen – einzuholen und von der Personalabteilung zu prüfen:

- Zeugnisse (dienstlich) und ggf. persönliche Referenzen.
- Ein auf Vollständigkeit und Richtigkeit geprüfter Lebenslauf des Bewerbers inklusive Bestätigung der akademischen und beruflichen Qualifikationen.
- Identitätsnachweise (Reisepass oder ähnliches Dokument).
- ggf. Nachweise zur Bestätigung der Zuverlässigkeit (z. B. ein Führungszeugnis).
- ggf. weitere Nachweise zur Zuverlässigkeit, sofern rechtlich zulässig und angemessen mit Blick auf die jeweils zu besetzende Funktion und die damit verbundenen Risiken.
- ggf. weitere regulatorisch geforderte Nachweise (z. B. bei Schlüsselfunktionen).

Die Prüfung der fachlichen Eignung des Bewerbers obliegt dem zuständigen Fachbereich (der Führungskraft).

Sofern eine Person für eine bestimmte Rolle der Informationssicherheit[1] angestellt wird, ist der einstellende Fachbereich dafür verantwortlich sicherzustellen, dass der Bewerber

1. über die notwendige Kompetenz für die Sicherheitsaufgabe und
2. über die erforderliche Vertrauenswürdigkeit verfügt, insbesondere wenn die Rolle von entscheidender Bedeutung für das Unternehmen ist.

Die eingereichten Unterlagen der Bewerber müssen im Einklang mit den rechtlichen Vorgaben von der Personalabteilung sicher verwahrt werden. Die Wahrung der Vertraulichkeit, die Beachtung des Zweckbindungsgrundsatzes sowie die Verpflichtung zur Datenlöschung gilt auch für die Fachbereiche, sollten diese Bewerbungsunterlagen zur Prüfung erhalten.
Im Zusammenhang mit der Aufnahme der Tätigkeit sind die Mitarbeiter mindestens über folgende Aspekte aufzuklären:

- Einhaltung der Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation.
- Wahrung der Vertraulichkeit von Informationen, die ihnen im Rahmen ihrer Tätigkeiten zugänglich sind (Geheimhaltung); dies gilt auch über das Beschäftigungsverhältnis hinaus.
- Regelungen der Datenschutz-, IT-Sicherheits- und Informationssicherheitsrichtlinien, sowie über die relevanten gesetzlichen Regelungen (z. B. Datenschutzgrundverordnung).

Es liegt in der Verantwortung der jeweiligen Führungskraft, dass der Erhalt von IT-Arbeitsmitteln und Authentisierungsmittel je Mitarbeiter dokumentiert wird und der Mitarbeiter den Erhalt bestätigt.

3.2. Vertragsbedingungen

In den vertraglichen Vereinbarungen (Arbeitsverträgen) sollten die Verantwortlichkeiten des Bewerbers näher spezifiziert werden. Die Arbeitsvertragsregelungen müssen insbesondere folgende Aspekte enthalten:

- Hinweis auf die Wahrung der Vertraulichkeit / Geheimhaltung.
- Hinweis auf die bestehenden gesetzlichen Verpflichtungen (z. B. zur Einhaltung des Datenschutzes).
- Allgemeiner Hinweis auf die anzuwendenden, relevanten Richtlinien.

3.3. Funktionstrennung

Bei der Besetzung von Positionen ist ferner darauf zu achten, dass es zu keiner Kombination von sogenannten „unvereinbaren Tätigkeiten“ kommt[2]. Generell ist darauf zu achten, dass operative Tätigkeiten von überwachenden Funktionen organisatorisch und personell getrennt werden.

[1] Rollen der Informationssicherheit sind solche, die unmittelbar Einfluss auf die Sicherheit der VAV ausüben. Dies sind z. B. Mitarbeiter der IT-Security, Infrastruktur-Administratoren, Mitarbeiter Wachdienst etc.

[2] So kann beispielsweise der Leiter der Revision nicht gleichzeitig der Leiter Vertrieb sein, der Administrator nicht der Logging-/ Protokollierungsbeauftragte, Debitoren- und Kreditorenbuchhalter etc.

4. WÄHREND DER BESCHÄFTIGUNG

4.1. Einarbeitung

Die Führungskraft ist für die Einarbeitung des neuen Mitarbeiters verantwortlich. Ein strukturierter Einarbeitungsplan stellt sicher, dass neue Mitarbeiter alle erforderlichen Informationen erhalten, um die Aufgaben nach der Einarbeitung sicher und fehlerfrei wahrnehmen zu können. Die Führungskraft hat darauf hinzuwirken, dass der Mitarbeiter über das notwendige Datenschutz- und Informationssicherheitsbewusstsein verfügt und ihm die für seinen Bereich geltenden Richtlinien bekannt sind. Der Mitarbeiter hat an den Pflichtschulungen teilzunehmen und die Teilnahmebestätigung ist aufzubewahren.

4.2. Organisierte Arbeitsabläufe

Die Führungskraft hat dafür Sorge zu tragen, dass jeder Mitarbeiter (gleiche Tätigkeiten können zusammengefasst werden) über eine Stellen- und Funktionsbeschreibung verfügt, die von der Führungskraft freigegeben und unterzeichnet ist. Die Führungskraft ist ferner für angemessene Ablaufbeschreibungen (Arbeitsrichtlinien etc.) im eigenen Bereich verantwortlich. Stellvertretungsregelungen sind zu dokumentieren. Gleiches gilt für Zeichnungsrechte und Vollmachtenrahmen, die beim Rechnungswesen zu hinterlegen und regelmäßig zu überprüfen sind. Für die Vergabe und Pflege von Rollen und Berechtigungen wird auf die „Arbeitsrichtlinie Zugangssteuerung“ verwiesen.

4.3. Schulungen und Sensibilisierungen

Alle Mitarbeiter sollten über ein angemessenes Informationssicherheitsbewusstsein verfügen. Schulungen und Sensibilisierungen zur Informationssicherheit erfolgen durch den Informationssicherheitsbeauftragten bzw. eine von ihm beauftragte Person. Schulungen zum Datenschutz erfolgen durch den Datenschutzbeauftragten oder in Abstimmung mit diesem.
Die Schulungsmaßnahmen sollten im Einklang mit den bestehenden Richtlinien und Vorgaben stehen sowie auf Basis eines Schulungskonzepts erfolgen, welches die Zielgruppen und Schulungsintervalle für das Unternehmen definiert. Das Schulungskonzept sollte unter Berücksichtigung der Aufgaben der Beschäftigten und unter Berücksichtigung der unternehmensinternen Erwartungen erfolgen sowie unterschiedliche Schulungsformen beinhalten. Die Schulungen und Sensibilisierungen sollten in einem angemessenen Zeitraum wiederholt werden. Im Falle von Pflichtschulungen ist die Teilnahme der Mitarbeiter – möglichst elektronisch – zu dokumentieren und diese Dokumentation an die Personalabteilung weiterzugeben. Wissenstests am Ende der Schulung fördern das Verständnis der Mitarbeiter und sind daher wünschenswert.

4.4. Maßregelungsprozess

Ein Verstoß eines Mitarbeiters gegen die Regelungen der Informationssicherheit und des Datenschutzes erfordert stets eine Einzelfallprüfung durch die Personalabteilung. Bei Feststellen eines Verstoßes sind geeignete, der Art und Schwere des Verstoßes angemessene Maßnahmen zu ergreifen.

5. AUSSCHEIDEN VON MITARBEITERN ODER ÄNDERUNG DER BESCHÄFTIGUNG

Auch nach einem Ausscheiden eines Mitarbeiters (gleich aus welchem Grund) sowie bei einem Wechsel eines Aufgabenbereiches sind Aspekte der Sicherheit zu beachten. Die Führungskräfte haben hierbei folgendes sicherzustellen:

- Unverzügliche, schriftliche Aufforderung des Mitarbeiters zur Rückgabe von Karten, Laptops, SIM Karten, Mobiltelefonen, Firmenwagen und sonstigen an den Mitarbeiter ausgehändigten Werten, die im Eigentum der VAV stehen. Nach Erhalt steuert die Führungskraft die Rückgabe an die jeweils zuständige Stelle (unter Einbindung des IT Supports bzw. des Facility Management).
- Löschung des Accounts des Mitarbeiters nach Ausscheiden und Aufforderung entsprechend der Vorgaben im IT Support.
- Löschung von Berechtigungen in Anwendungen/Systemen, die nichtzentral verwaltet werden.
- Vernichtung von Unterlagen in den Datenschutzcontainern, sofern keine Aufbewahrungsfristen oder betrieblichen Notwendigkeiten zur Vorhaltung bestehen.

Bei Vorliegen von Gründen (insbesondere Entlassungsgründen), die eine Gefahr für die Informationssicherheit oder den Datenschutz darstellen, sind obige Punkte unverzüglich sicherzustellen.
Zur Gewährleistung des ordnungsgemäßen Austritts eines Mitarbeiters steht die „Checkliste Austritt“ zur Verfügung.