Arbeitsrichtlinie Betriebssicherheit

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Betriebssicherheit
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	16.10.2019
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	16.10.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Änderungen in Kap 2.6 (Konkretisierung unbekannter Quellen und Berücksichtigung betrieblicher Abhängigkeiten bei Außerbetriebnahme) in Anlehnung an die Arbeitsrichtlinie der VHV in der Version 20.0	Daniel Fürdauer
21.0	22.11.2021	Änderungen in Kap 1 und 2.2 (Aufnahme von Cloudumgebungen; Konkretisierung Netzzonen) in Anlehnung an die Arbeitsrichtlinie der VHV in der Version 21.0	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 von Informationssicherheit sind neben technischen Aspekten auch organisatorische Aspekte zu beachten, um einen sicheren und ordnungsgemäßen IT-Betrieb zu gewährleisten. Daneben sind betriebliche Anforderungen zu beachten, um IT-Systeme und die in diesem Zusammenhang verarbeiteten Daten über den gesamten Lebenszyklus hinweg zu schützen. Dies gilt auch in Cloudumgebungen, sofern anwendbar. Diese organisatorischen Anforderungen sind in dieser Richtlinie geregelt.

2. ALLGEMEINE ANFORDERUNGEN

2.1. Betriebsverfahren

Betriebsverfahren und Abläufe sind in einem Betriebsdokument zu beschreiben, sodass auch fachkundige Dritte anhand der Beschreibung den Betrieb sicherstellen können. Folgende Mindestangaben sind hierbei zu berücksichtigen:

- Installations- und Konfigurationseinstellungen,
- Verfahren und Abhängigkeiten bei Neustarts,
- Umgang mit Datensicherungen,
- Einspielen von Sicherheitspatchen,
- Sicherung und Speicherort der Konfigurationsparameter,
- Vergabe und Pflege von administrativen Berechtigungen,
- Anbindung an das Managementnetz,
- Absicherung des administrativen Zugriffs.

2.2. Netzzonen

IT-Systeme dürfen nur in dafür vorgesehenen Netzzonen betrieben werden. So sind Entwicklungssysteme im Entwicklungsnetz und Testsysteme im Testnetz zu verorten. Nur Produktivsysteme dürfen im Produktionsnetz betrieben werden. Im Produktionsnetz sind Produktivsysteme entsprechend ihrer Funktion in den dafür vorgesehenen Netzzonen zu verorten.

2.3. IT-Systeme und technische Arbeitsmittel

Nicht von der VAV freigegebene IT-Systeme und technische Arbeitsmittel[1] dürfen nicht genutzt oder mit den VAV Systemen vernetzt werden. Die Vernetzung betriebsfremder IT-Systeme und technischer Arbeitsmittel ist technisch (nach dem Stand der Technik) zu unterbinden. Eine Ausnahme besteht für die VPN-Einwahl in das VAV-Netz zur Nutzung der Citrix Umgebung mittels eines fremden Gerätes.

2.4. Software

Es sind Maßnahmen zu ergreifen, um die Nutzung unberechtigter Software zu erkennen und zu verhindern.

[1] Technische Arbeitsmittel: z. B. Smartphone, externe Festplatte, USB-Stick

2.5. Administrationswerkzeuge

Es sind grundsätzlich systeminterne Administrationswerkzeuge zu verwenden. Sofern durch ein IT-System keine geeigneten systeminternen Administrationswerkzeuge bereitgestellt werden, sind zunächst Werkzeuge zu nutzen, die bereits innerhalb der IT freigegeben wurden. Die Nutzung nicht freigegebener Administrationswerkzeuge ist untersagt.
Maßnahmen zur Nutzung von administrativen Werkzeugen sind in der „Arbeitsrichtlinie Zugangssteuerung“ zu entnehmen.

2.6. Skripte und ausführbare Dateien

Die Erstellung und Nutzung von Skripten und ausführbaren Dateien jeglicher Art (zum Beispiel: Batch-Dateien, Makros, selbstentwickelte Datenbanken, Skripte und sonstige Arten von automatisierten Verfahren zum Aufrufen mehrerer Kommandobefehle nacheinander) darf ausschließlich zur Administration von IT-Systemen erfolgen.
Beim Einsatz von Skripten sind die folgenden Vorgaben verbindlich einzuhalten:

- Skripte sind aus sicheren Quellen[2] zu beziehen.
- Es dürfen ausschließlich die in der Informatik bereitgestellten Werkzeuge zur Erstellung von Skripten genutzt werden.
- Es dürfen nur Mitarbeiter für die Erstellung und Nutzung von Skripten eingesetzt werden, die dazu durch entsprechende fachliche Qualifikation befähigt sind.
- Skripte sind vor ihrem Einsatz ausführlich vom zuständigen Mitarbeiter zu testen. Für die Tests dürfen keine Produktivdaten verwendet werden. Die Tests können allerdings auf Produktivsystemen durchgeführt werden, sofern keine Alternativen bereitstehen, eine Risikoabschätzung erfolgt und der Test genehmigt ist.
- Skripte sind stets durch den Ersteller in für fachkundige Dritte verständlicher Form zu dokumentieren. Die Dokumentation muss mindestens folgende Inhalte umfassen: Aktualität, Funktionsweise, Schnittstellen, Verwendung und Zweck. Diese Dokumentation muss Bestandteil des Headers der Skriptdatei sein.

2.7. Asset- und Configuration-Management

Es ist sicherzustellen, dass ein aktueller Überblick über die Bestandteile des festgelegten Informationsverbunds sowie deren Abhängigkeiten und Schnittstellen besteht.
Zu einem Informationsverbund gehören insbesondere die geschäftsrelevanten Informationen, Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen. Die Verantwortlichkeit zur Erfassung der geschäftsrelevanten Informationen sowie der Geschäftsprozesse liegt in den Fachbereichen.
Des Weiteren sind die Komponenten der IT-Systeme sowie deren Beziehungen zueinander in geeigneter Weise zu verwalten und die hierzu erfassten Bestandsangaben sind regelmäßig sowie anlassbezogen zu aktualisieren.
Zu den Bestandsangaben zählen insbesondere:

- Beschreibung und Verwendungszweck der Komponenten der IT-Systeme mit den relevanten Konfigurationsangaben,
- Standort der Komponenten der IT-Systeme,

[2] Als sichere Quelle gelten insbesondere Seiten von Herstellern und von Herstellern moderierte Foren.

- Aufstellung der relevanten Angaben zu Gewährleistungen und sonstigen Supportverträgen,
- Angaben zum Ablaufdatum des Supportzeitraums der Komponenten der IT-Systeme,
- akzeptierter Zeitraum der Nichtverfügbarkeit der IT-Systeme sowie der maximal tolerierbare Datenverlust, jedenfalls sofern sie BCM-relevant sind.

3. ANFORDERUNGEN WÄHREND DES LIFECYCLES

3.1. Inbetriebnahme

Vor Inbetriebnahme eines IT-Systems ist sicherzustellen, dass die definierten funktionalen und nicht funktionalen Anforderungen unter Beachtung der bestehenden Richtlinien und Regelprozesse umgesetzt werden.

3.2. Während des Betriebs

Im Betrieb sind die Incident-, Problem-, Change- und Patch Management Prozesse zu durchlaufen. Insbesondere sind während des Betriebs Änderungen hinreichend zu planen, zu testen und zu dokumentieren. Ebenso sind erforderliche Anpassungen an die benötigten Ressourcen und Kapazitäten einzuplanen und umzusetzen.
Aktualisierungen dürfen erst nach erfolgreichem Test produktiv gesetzt werden. Die Aktualisierungen sind vorher auf Datenschutz und IT-Sicherheitsaspekte zu prüfen und bei Relevanz durch die Stabstelle Datenschutz und Informationssicherheit bewerten zu lassen. Die Umsetzung muss durch geschultes Personal erfolgen.

3.3. Außerbetriebnahme

Die Außerbetriebnahme soll sicher und nachvollziehbar erfolgen.
IT-Systeme, die vom Hersteller nicht mehr mit Sicherheitspatches versorgt werden, sind zeitnah, unter Berücksichtigung von betrieblichen Abhängigkeiten, außer Betrieb zu nehmen.
Bevor der Hersteller die Versorgung mit Sicherheitspatches einstellt, ist die Außerbetriebnahme so zu planen, dass der Betrieb des IT-Systems vier Wochen nach Veröffentlichung des letzten Sicherheitspatches oder Abkündigung durch den Hersteller eingestellt wird. Ist eine Außerbetriebnahme nicht möglich, muss das IT-System durch zusätzliche mit Stabstelle Datenschutz und Informationssicherheit abzustimmende Schutzmaßnahmen, unter Berücksichtigung von betrieblichen Abhängigkeiten, isoliert werden.
Falls das IT-System nicht mehr benötigt wird, ist dafür Sorge zu tragen, dass alle Daten, die aufbewahrungspflichtig sind, archiviert werden. Anschließend sind alle Daten unwiderruflich zu löschen. Die Löschung liegt in der Entscheidungsverantwortung des Informationseigentümers. Ebenfalls sind Kommunikationsbeziehungen in den Regelwerken zu löschen.
Wird ein IT-System erneuert, sind die erforderlichen Daten und Konfigurationsparameter, sofern erforderlich, auf das neue IT-System zu übertragen. Während der Übertragung ist sicherzustellen, dass Unbefugte keine Kenntnis von den Daten erlangen. Anschließend sind auf dem Altsystem alle Daten unwiderruflich zu löschen.