

Amtliche Verlautbarung der österreichischen Sozialversicherung im Internet

Hauptverband der österreichischen Sozialversicherungsträger

Der Hauptverband der österreichischen Sozialversicherungsträger verlautbart gemäß § 31 Abs. 5 Z 4 ASVG:

Sicherheitsrichtlinie für die gesetzliche Sozialversicherung (SV-Sicherheitsrichtlinie 2019 – SV-SR 2019)

Geltungsbereich

§ 1. (1) Diese Richtlinie gilt für alle dem Hauptverband der österreichischen Sozialversicherungsträger angehörenden Sozialversicherungsträger und den Hauptverband selbst. Sie ist auch für die Vorgangsweise jener Organisationseinheiten zu beachten, über die ein Sozialversicherungsträger oder der Hauptverband

1. eine Aufsicht wie über eine eigene Dienststelle ausübt (z. B. in-house Gesellschaften nach § 10 BVergG 2018),
2. aus anderen Gründen maßgebenden Einfluss besitzt oder
3. die Rolle eines von mehreren gemeinsamen Verantwortlichen nach Art. 26 DSGVO inne hat,

(z. B. Tochtergesellschaften wie ITSV, SVC u.a., alle im Folgenden „SV-Organisationen“ genannt). Der im Folgenden verwendete Begriff „SV-weit“ bezieht sich auf alle SV-Organisationen. Er gilt auch für unselbstständige Organisationseinheiten, die von einer oder mehreren SV-Organisationen geführt werden (Competence Center, z. B. nach § 5 Abs. 1 Z 1 REDV 2006).

(2) Die Verantwortung eines Sozialversicherungsträgers für die Vollziehung der ihm gesetzlich übertragenen Aufgaben und die Verantwortung seiner Organe werden durch diese Richtlinie nicht verändert.

Zweck

§ 2. (1) Zweck dieser Richtlinie ist eine für alle SV-Organisationen einheitliche Vorgangsweise bei folgenden Sicherheitsthemen zu erreichen:

1. Risikomanagement der Informationssicherheit
2. Informationssicherheit
3. Krisenmanagement

(2) Die Erbringung der Dienstleistungen der Sozialversicherung erfordert ein hohes Maß an Risikobewusstsein. Dazu ist ein SV-weites, koordiniertes Vorgehen einzuhalten. Alle SV-Organisationen sind verpflichtet, ihre Risiken mittels eines Risikomanagement-Prozesses zu steuern. Dafür sind, entsprechend dem Stand der Technik, gemeinsame SV-weite Mindeststandards und Methoden umzusetzen. Diese orientieren sich am nationalen Standard Risikomanagement für Organisationen und Systeme (ONR 49000 ff., in späterer Folge ON D 4900 ff.) und am internationalen Standard Risikomanagement (ISO 31000) in ihrer jeweils gültigen Fassung.

(3) Die in der Sozialversicherung bearbeiteten Daten erfordern ein hohes Maß an Informationssicherheit. Das wird in der „Informationssicherheitsstrategie der österreichischen Sozialversicherung“ genauer beschrieben.

(4) Die Dienstleistungen der Sozialversicherung erfordern ein hohes Maß an Verfügbarkeit. Dazu wird ein SV-weites Krisenmanagement benötigt, das durch diese Richtlinie strategisch vorgegeben und in einer detaillierten Handlungsanleitung genauer beschrieben wird. Die SV-Organisationen haben sich bei Eintritt einer SV-weiten Krise zur Einhaltung der vereinbarten Handlungsweise verpflichtet. Die SV-Organisationen orientieren sich zur Sicherstellung ihrer Funktionsfähigkeit im Krisenfall am österreichischen staatlichen Krisen- und Katastrophenschutzmanagement (SKKM).

Risikomanagement der Informationssicherheit

§ 2a. (1) Das Risikomanagement dient unter anderem dazu, geschäftskritische Prozesse aufzuzeigen, Gefahren und Bedrohungen zu bewältigen, und bietet gleichzeitig die Möglichkeit Chancen zu nutzen.

(2) Der Hauptverband hat ein Risikomanagementhandbuch (SV-RM-Handbuch) auszuarbeiten und aktuell zu halten. Das SV-RM-Handbuch hat SV-weite Mindeststandards, Methoden und Begriffsdefinitionen zu enthalten. Diese Unterlage ist der Trägerkonferenz in ihrer jeweils aktuellen Form auf derselben technischen Ebene wie Sitzungsunterlagen zugänglich zu machen, um Gelegenheit zu geben, allfällige Änderungen vorzuschlagen und zu diskutieren. Aktualisierungen sind vom Hauptverband zu initiieren.

§ 2b. (1) Jede SV-Organisation hat Vorgaben auf Basis des SV-RM-Handbuches zu erstellen und aktuell zu halten. Diese haben zu beinhalten:

1. Beschreibung des Risikomanagementsystems
2. Beschreibung des Risikomanagementprozesses
3. Dokumentation und Kommunikation des Risikomanagements

Informationssicherheit

§ 3. (1) Informationssicherheit steht in der Verantwortung der gesamten Sozialversicherung und kann nur organisationsübergreifend und SV-weit gewährleistet werden. Sie umfasst den Schutz aller Informationen, die in jeglicher Form erfasst, verarbeitet, übertragen, gespeichert, archiviert, gelöscht oder entsorgt werden. Oberstes Ziel ist es, die Vertraulichkeit, Integrität, Verfügbarkeit und ebenso die Verbindlichkeit und Authentizität von Informationen zu gewährleisten.

(2) Eine „Informationssicherheitsstrategie der österreichischen Sozialversicherung“ (SV-Informationssicherheitsstrategie) mit Zielsetzungen, Mindeststandards und Empfehlungen für eine effektive, effiziente und nachhaltige Informationssicherheit in der österreichischen Sozialversicherung ist zu definieren. Der Hauptverband hat auf der Grundlage des für den Bereich des Bundes erstellten österreichischen Informationssicherheitshandbuchs über die CISO Community diese samt mitgeltenden Dokumenten (detaillierte Mindeststandards für die einzelnen Sicherheitsthemen) zu erstellen, weiterzuentwickeln und aktuell zu halten. Diese Unterlagen sind der Trägerkonferenz in ihrer jeweils aktuellen Form auf derselben technischen Ebene wie Sitzungsunterlagen zugänglich zu machen, um Gelegenheit zu geben, allfällige Änderungen vorzuschlagen und zu diskutieren. Aktualisierungen sind vom Hauptverband zu initiieren.

(3) Die SV-Informationssicherheitsstrategie wird mit der Beschlussfassung durch die Trägerkonferenz für die SV-Organisationen SV-weit verbindlich und ist somit umzusetzen. Widersprüche in anderen Regelwerken sind an die Regelungen dieser Informationssicherheitsstrategie der österreichischen Sozialversicherung anzupassen.

(4) Die in der SV-Informationssicherheitsstrategie und in den mitgeltenden Dokumenten angeführten Mindeststandards sind zumindest alle drei Jahre initiiert durch den Hauptverband der Sozialversicherungsträger zu überprüfen.

(5) Die mitgeltenden Dokumente der SV-Informationssicherheitsstrategie (wie zum Beispiel Handlungsanleitungen und Handbücher) müssen durch die SV-Organisationen in internen Sicherheitsvorgaben (zum Beispiel Dienstabweisungen) verbindlich gemacht werden.

(6) Zur Erkennung der relevanten Informationssicherheitsrisiken evaluiert jährlich jede SV-Organisation ihr lokales Informationssicherheitsbild und stellt dabei fest, ob die Mindeststandards der SV-Informationssicherheitsstrategie erfüllt werden und ausreichend sind. Risikoreaktionen müssen auf Basis von Analyse von Sicherheitsvorfällen und der jährlichen Evaluierung des lokalen Informationssicherheitsbilds erarbeitet und umgesetzt werden.

(7) Jährlich ist das lokale Informationssicherheitsbild der SV-Organisationen an die CISO Community zu melden, von dieser anonymisiert in einem SV-Sicherheitsgesamtbild zusammenzufassen und an die Trägerkonferenz zu berichten. Der Bericht hat bei Bedarf auch Vorschläge der CISO Community zur Verbesserung der SV-weiten Informationssicherheit zu enthalten.

Organisationsstrukturen der Informationssicherheit

§ 4. (1) Um den in § 2 Abs. 3 angeführten Zweck zu erreichen, sind folgende Organisationseinheiten einzurichten:

1. Bei allen SV-Organisationen ist die Rolle eines CISO (Chief Information Security Officer) als zentrale Stelle für Anfragen, Ideen oder Verbesserungen zur Informationssicherheit einzurichten.
2. Die CISO Community wird als beratendes Gremium der Trägerkonferenz auf dem Gebiet der Informationssicherheit durch den Hauptverband eingesetzt. Jede SV-Organisation hat Teilnehmer zur CISO Community zu nominieren.
3. Das SV-CERT („Computer Emergency Response Team“ der österreichischen Sozialversicherung) wird durch den Hauptverband eingesetzt und berät und unterstützt die SV-Organisationen auf dem Gebiet der Informationssicherheit.

(2) Der Chief Information Security Officer (CISO) ist Mitglied der CISO Community.

(3) Die CISO Community ist ein beratendes Organ der Trägerkonferenz auf dem Gebiet der Informationssicherheit. Sie besteht aus den CISOs aller SV-Organisationen. Die CISO Community hat sich mit der Optimierung der SV-weiten Informationssicherheit, insbesondere mit folgenden Themen zu befassen:

1. Bedrohungen und Gegenmaßnahmen zur allgemeinen Computersicherheit und Cyber-Sicherheit.
2. geschäftskritischer Informations- und Kommunikations-Technologie in der Sozialversicherung.
3. Dokumentation und Beurteilung relevanter Informationssicherheitsrisiken und Initiierung der Erarbeitung geeigneter Risikoreaktionen bei fachlich Verantwortlichen.
4. Erstellung eines Informationssicherheitsberichtes mindestens einmal pro Jahr, in dem SV-weit das Gesamtbild der Informationssicherheit darzustellen und der Status der Risikoreaktionen zu dokumentieren ist.
5. Informationsaustausch zwischen den CISOs, um das vorhandene Wissen zum Thema Informationssicherheit einzelner SV-Organisationen SV-weit zugänglich zu machen.
6. Förderung des gegenseitigen Vertrauens der CISOs, damit bei Informationssicherheitsvorfällen rasch und umfassend Information ausgetauscht werden kann und Förderung des Lernens aus Informationssicherheitsvorfällen.
7. Erarbeitung von Vorschlägen für SV-weite Prozesse zu Themen der Informationssicherheit wie z. B. Business Continuity Management (BCM).
8. Erarbeitung von SV-weit geltenden Mindeststandards für Informationssicherheit.

SV-Sicherheitsrichtlinie (SV-SR)

9. Initiierung von Angeboten an Schulungen und Abhaltung von Fachveranstaltungen über Entwicklungen auf den Gebieten Informationssicherheit, Risikomanagement, Krisenmanagement und Cyber-Sicherheit, um den erforderlichen Wissensstand in der SV, insbesondere der CISOs zu erreichen, bzw. zu halten.

(4) Aufgabe des SV-CERT („Computer Emergency Response Team“ der österreichischen Sozialversicherung) ist es, innerhalb der Sozialversicherung Dienste bereitzustellen, die es ermöglichen, rasch auf Cyber-Bedrohungen zu reagieren und entsprechende Präventivmaßnahmen umzusetzen, sowie im Schadensfall entsprechende Untersuchungen durchzuführen und bei der Behebung zu unterstützen. Die Aufgaben des SV-CERT sind:

1. Zentrale Meldestelle für eingetretene oder vermutete Informationssicherheitsvorfälle sowie Weiterleitung von Alarm- und Warnmeldungen an potentiell betroffene SV-Organisationen.
2. Sammeln von externen Sicherheitsinformationen, Prüfen auf Relevanz für die SV-Organisationen und Warnen der potentiell betroffenen SV-Organisationen.
3. Unterstützung bei der Identifikation, Analyse und Behebung von Sicherheitsvorfällen, wie Beweissicherung, forensischen Analysen, sowie Unterstützung bei der Beseitigung von Schadsoftware.
4. Anbieten von Sicherheitswerkzeugen zur Analyse und Behebung von Schadsoftware für die SV-Organisationen.
5. Anbieten von Schwachstellenüberprüfungen von Systemen durch Spezialisten des SV-CERT.
6. Unterstützung der SV-Organisationen bei Awareness-Maßnahmen.

SV-Krisenmanagement

§ 5. Der Hauptverband hat detaillierte Handlungsanleitungen (SV-BCM-Handbuch) auszuarbeiten und aktuell zu halten. Diese Unterlagen sind der Trägerkonferenz in ihrer jeweils aktuellen Form auf derselben technischen Ebene wie Sitzungsunterlagen zugänglich zu machen, um Gelegenheit zu geben, allfällige Änderungen vorzuschlagen und zu diskutieren. Aktualisierungen sind vom Hauptverband zu initiieren.

Definitionen

§ 6. (1) **Störfälle** sind Situationen, die den Betrieb (die Dienstleistungserbringung) beeinträchtigen oder unterbrechen. Sie werden im Rahmen der betriebsgewöhnlichen Strukturen (Linienorganisation) und Ressourcen durch betriebliche Maßnahmen behoben.

(2) **Notfälle** sind Situationen, die den Betrieb (die Dienstleistungserbringung) beeinträchtigen oder unterbrechen und sofortiges Handeln erfordern und bei denen unmittelbare Gefahr für Personen und Sachwerte droht. Der Notfall ist örtlich oder sachlich begrenzt und kann durch einen überdurchschnittlichen, meist bereichsübergreifenden Einsatz der bestehenden betrieblichen Ressourcen (Notfallteam, Task Force) und z. T. unter Zuhilfenahme externer Ressourcen bewältigt werden.

(3) **Krisen** sind Situationen, die organisationsweit außergewöhnliche Maßnahmen erfordern und nur mit besonderem Einsatz der Führungskräfte (Stabsarbeit) bewältigt werden können. Die Auswirkungen der Krise bedrohen Personen, Sachwerte, Umwelt und/oder das Ansehen der Organisation in der Öffentlichkeit. In der Sozialversicherung wird weiter unterschieden:

1. **Lokale Krise:** Krise in einer SV-Organisation
2. **Lokale Krise mit Außenwirkung:** Krise in einer SV-Organisation, von der andere SV-Organisationen betroffen sind, letztere aber maximal in den Notfall-Status kommen
3. **SV-weite Krise:** Krisen, bei denen mehr als eine SV-Organisation mit der gleichen oder ähnlichen Thematik den Krisenstatus erreicht oder der Hauptverband von sich aus eine SV-weite Krise ausruft

(4) **Katastrophen** sind Situationen, die von ihren Ursachen bzw. in ihrer Auswirkung über die SV-Organisationen weit hinausgehen und in denen eine effiziente Katastrophenhilfe nur durch Zusammenarbeit aller zuständigen Stellen des Bundes mit den Katastrophenschutzbehörden der Länder sowie den Hilfs- und Einsatzkräften bewältigt werden kann.

Organisationsstrukturen des SV-Krisenmanagements

§ 7. (1) Jede SV-Organisation hat ein festgelegtes Konzept zur Bewältigung von lokalen Krisen zu erstellen und aktuell zu halten. Dieses beinhaltet:

1. Die Führungsaufgaben im Krisenfall sind geklärt.
2. Der Handlungsspielraum des Krisenstabes im Krisenfall ist definiert, bekannt und ausreichend.
3. Die Verantwortung für Business Continuity Management in der Organisation ist festgelegt und beinhaltet:
 - a) Pflege der Dokumentation
 - b) Verfügbarkeit der Dokumentation
 - c) Risikoanalyse (Business Impact Analyse)
4. Vorsorgemaßnahmen sind getroffen und dokumentiert.
5. Das Konzept wird geschult und ist den potentiellen Krisenstabsmitgliedern bekannt.

(2) Mindestens einmal jährlich ist das lokale Krisenkonzept von jeder SV-Organisation einer konkret zu planenden Annahme eines Krisenfalles auch praktisch zu üben.

SV-Sicherheitsrichtlinie (SV-SR)

§ 8. (1) Jede SV-Organisation hat den Hauptverband sofort über die Ausrufung sowie über die Beendigung einer lokalen Krise zu informieren. Die Meldung wird durch bereits bestehende Strukturen durchgeführt.

(2) Das Ausrufen und Beenden einer SV-weiten Krise und die Einberufung des SV-Krisenstabes sind Aufgaben des Verbandsmanagements des Hauptverbandes. Der/Die Verbandsvorsitzende und der/die Vorsitzende der Trägerkonferenz sowie deren Stellvertreter/innen sind davon sofort zu informieren.

(3) Im Fall einer SV-weiten Krise ist ein Krisenstab einzusetzen, der die Gesamtsteuerung übernimmt (SV-Krisenstab). Alle SV-Organisationen haben dabei

1. bei SV-weiten Krisen und Katastrophen mit dem übergeordneten SV-Krisenstab zusammenzuarbeiten, bei Bedarf mitzuwirken und im Fall unterschiedlicher Entscheidungsalternativen dessen Entscheidungen zu akzeptieren.
2. für den Fall einer SV-weiten Krise mindestens einen Ansprechpartner zu definieren.
3. mit anderen Krisenstäben in standardisierter Form zu kommunizieren, wofür folgende Schnittstellen bzw. Informationen bereit zu stellen sind:
 - a) Einrichtung einer Kommunikationsschnittstelle (SKKM: „S6“)
 - b) Teilnahme der lokalen Einsatzleiter in Lagebesprechungen des SV-Krisenstabs zur Abstimmung wichtiger Entscheidungen
 - c) Erstellen von lokalen Lageberichten (SKKM: „S2“) und Übermittlung an den SV-Krisenstab
 - d) Erarbeiten von Handlungsalternativen (SKKM: „S3“) aus der Sicht der lokalen Organisation und Übermittlung an den SV-Krisenstab
4. zu dokumentieren, mit welchen Zielgruppen sie gegebenenfalls kommunizieren (Vorlage: Kommunikationsplan in den BCM-Unterlagen der CISO Community).
5. lokale Maßnahmen an den SV-weiten Entscheidungen auszurichten.
6. die vom SV-Krisenstab getroffenen Entscheidungen im lokalen Verantwortungsbereich umzusetzen und deren Durchführung zu bestätigen.

(4) Die im Abs. 3 angeführten Maßnahmen haben sicherzustellen, dass Entscheidungen rasch und mit dem bestmöglichen Wissensstand getroffen werden. Die Bedürfnisse der lokal betroffenen SV-Organisationen können dadurch bestmöglich in die Krisenbewältigung einbezogen werden.

(5) Bei SV-weiten Krisen ist die Kommunikation nach außen (z. B. Versicherte, Vertragspartner/innen, Medien, etc.) inhaltlich abzustimmen. Die letzte Entscheidung dazu hat der SV-Krisenstab.

(6) Für Entscheidungen im Krisenfall gilt für den SV-Krisenstab und allen SV-Organisationen die business-judgement-rule. Entscheidungen können nur auf Basis des Wissens zum konkreten Entscheidungszeitpunkt getroffen werden. Spätere Veränderungen können keine Vorwürfe begründen.

(7) Zur besseren Vorbereitung auf einen Ernstfall und zur Übung der Zusammenarbeit hat der Hauptverband einen Übungsplan zu erstellen und wiederkehrende SV-Organisationsübergreifende Krisenübungen anzuberaumen.

(8) Nach jeder Krise (Katastrophe) bzw. Übung sind organisationsintern – bei SV-weiten Krisen organisationsübergreifende – Evaluierungen durchzuführen (lessons learned-Veranstaltung), in denen Verbesserungspotentiale der Krisenvorsorge identifiziert werden und ihre Umsetzung veranlasst wird.

Schlussbestimmung

§ 9. (1) Diese Richtlinie tritt mit 1. Jänner 2019 in Kraft. Die Richtlinie SV-SR 2017, avsv Nr. 95/2017, und die erste Änderung zur SV-SR 2017, avsv Nr. 128/2018, treten mit 31. Dezember 2018 außer Kraft.

(2) Jede SV-Organisation muss bis spätestens 31. Dezember 2020 die in der SV-Informationssicherheitsstrategie angeführten Mindeststandards umsetzen. Abweichungen sind im lokalen Informationssicherheitsbild zu dokumentieren und die daraus entstehenden Risiken von der jeweiligen SV-Organisation zu tragen.

(3) Die erste Überprüfung nach § 3 Abs. 4 ist spätestens bis 31. Dezember 2019 durchzuführen.

(4) Jede SV-Organisation hat bis spätestens 31. Dezember 2020 die in § 2b angeführten Vorgaben umzusetzen.

*

Diese Richtlinie wurde in der Trägerkonferenz des Hauptverbandes der österreichischen Sozialversicherungsträger am 11. Dezember 2018 beschlossen. Die Erläuterungen dieser Richtlinie sind unter www.sozdok.at kostenlos zugänglich.

Für den Hauptverband der österreichischen Sozialversicherungsträger:

Reischl

Probst

