Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV
Direktionsstab DS – IT-Management ITM

eGov-Mitteilung Nr. 053 vom 17.12.2024

Geht an: - Durchführungsstellen der 1. Säule/FamZ
- - IT-Pools

Betreff: - Anpassungen der Weisungen W-ISDS und WAID
- Meldepflicht bei Cybervorfällen und Beeinträchtigungen der Informationssysteme

1 Anpassungen der Weisungen W-ISDS und WAID

In den Weisungen W-ISDS wurden keine Anforderungen substanziell verändert. Sie wurden jedoch redaktionell so überarbeitet, dass sie klarer und verständlicher sind. Diese Anpassungen wurden in enger Abstimmung mit der Betriebsgruppe BEWIA[1] umgesetzt. Unter anderem wurden die Gültigkeit von Prüfberichten nach ISO 27001 und ISAE 3000 neu festgelegt und die Anhänge in der W-ISDS auf den neuesten Stand gebracht. Zudem wurde der neue Meldeprozess für Cybervorfälle nach BPMN[2]-Standard modelliert.

Bezüglich der Verwendung von M365 und der Speicherung und Bearbeitung von besonders schützenswerten Daten bei einem Cloud-Provider kann zum jetzigen Zeitpunkt noch keine neue Aussage gemacht werden, da das Thema innerhalb vom BSV noch nicht abschliessend behandelt wurde. Somit gelten wie bis anhin die Cloud-Prinzipien der Bundesverwaltung in der W-ISDS. Im Laufe des ersten Quartals 2025 wird das BSV eine aktualisierte Information zum Thema M365 und Public Clouds veröffentlichen.

Die wesentlichen Änderungen im Überblick:

W-ISDS Weisungen über die Anforderungen an die Informationssicherheit und den Datenschutz der Informationssysteme der Durchführungsstellen der 1. Säule/FamZ	• Mapping der Anforderungen auf die ISO-Norm 27001:2022 angepasst (gültige Version vom 1.1.2024 basierte auf ISO 27001:2013). • Gültigkeit von ISO- und ISAE-Prüfberichte als Randziffer 1.6 neu festgelegt. • Aufteilung der Randziffer 2.15: - 2.15.1 Verträge mit Dritten (allgemein) - 2.15.2 Cloud-Prinzipien der Bundesverwaltung • Neuer «Meldeprozess Sicherheitsvorfall» als Anhang 2 hinzugefügt. • ISDS-Basisdokumentation (Anhang 3) bezüglich Schutzbedarfsanalyse mit

[1] BEWIA: Betriebsgruppe Weisungen W-ISDS und IT-Audits
[2] BPMN: Business Process Model and Notation (Modell und Notation für Geschäftsprozesse)

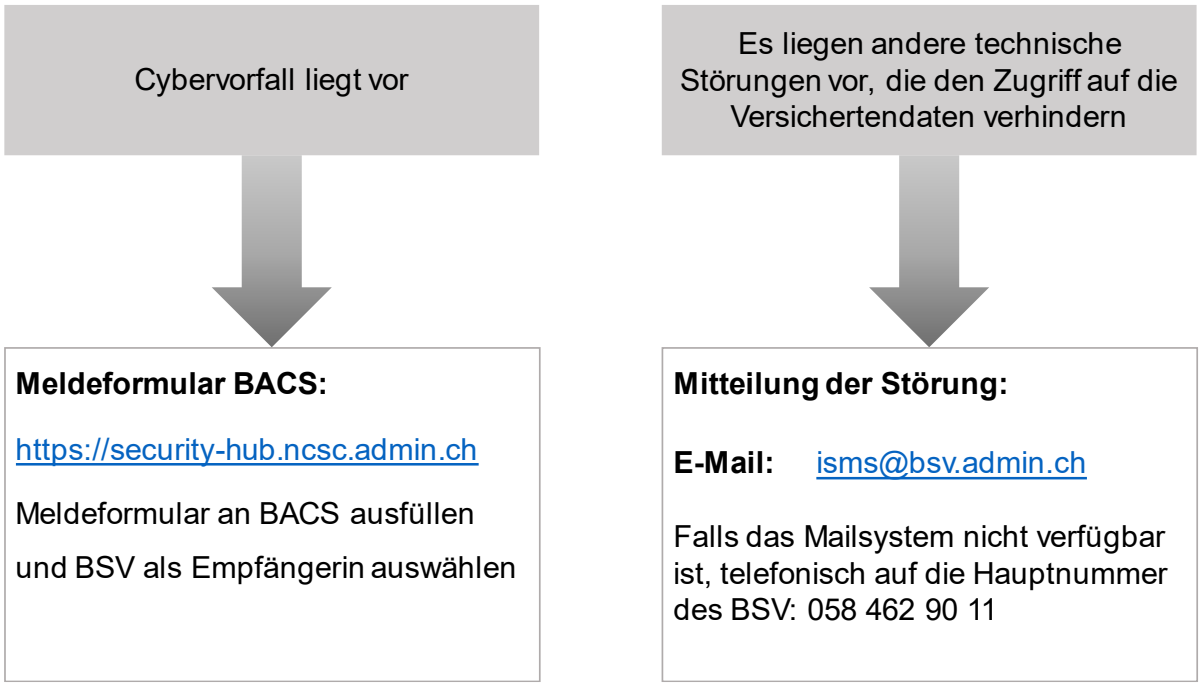
	Diagramm ergänzt und ein Beispiel von Schutzgruppen hinzugefügt. • Zusammenstellung der Rollenanforderungen an die Durchführungsstellen (Anhang 5) hinzugefügt. • Links zu Hilfsmittel und Vorlagen (Anhang 6) hinzugefügt
WAID Weisungen zu den Audits über die Informationssicherheit und den Datenschutz	• Kapitel 2.2 Auditierte Stellen, Randziffer 7: Gültigkeit ISAE-Prüfberichte hinzugefügt. • Kapitel 2.5, Randziffer 14: Beschreibung vom Scope des IT-Audits bei Vorlage eines gültigen ISO 27001 / ISAE-Prüfberichts. • Anhang 2: Fragebogen IT-Audit: Mapping auf ISO-Norm 27001:2022 geändert.

2 Meldepflicht bei Systembeeinträchtigungen (Rz 2.3 W-ISDS)

Gemäss Randziffer 2.3 W-ISDS, sollen die Durchführungsstellen über ein Informationssicherheitsvorfall-Bearbeitungsprozess verfügen. Die Meldepflicht gemäss Artikel 141^{septies} der Verordnung über die Alters- und Hinterlassenenversicherung (AHVV), gilt für alle Durchführungsstellen der 1. Säule. Es ist die Aufgabe des BSV als materielle Aufsichtsbehörde, darüber informiert zu werden, ob die gesetzlichen Aufgaben von den Durchführungsstellen korrekt erfüllt werden können. Die Informationssysteme der Durchführungsstellen gehören gemäss Informationssicherheitsgesetz (ISG) zu den kritischen Infrastrukturen. Daher müssen Cybervorfälle auch dem Bundesamt für Cybersicherheit (BACS) gemeldet werden. Die Meldung eines Cybervorfalls erfolgt mit demselben Formular wie die Meldungen ans BSV. Liegen anderweitige technische Störungsgründe (kein Cybervorfall) vor, welche den Zugriff auf die Versichertendaten beeinträchtigen oder verhindern, sind diese unverzüglich dem BSV über einen direkten Kanal (siehe Abschnitt 3: «Meldung von Systembeeinträchtigungen auf einen Blick») zu melden. So kann das BSV die Durchführungsstellen unterstützen, falls sich Versicherte direkt an das BSV wenden.

- Das neue Meldeformular bei Cybervorfälle wird gemäss BACS ab dem 1. April 2025 über den «Cyber Security Hub» (https://security-hub.ncsc.admin.ch) verfügbar sein.
- Das BSV informiert, sobald das Formular vom BACS zur Verfügung steht. Bis dahin müssen die Meldungen an das BSV per E-Mail an isms@bsv.admin.ch eingereicht werden.

3 Meldung von Systembeeinträchtigungen auf einen Blick



Wir danken Ihnen für Ihre Kenntnisnahme.

Bereich DS/IT-Management