

Weisung 202310005 vom 20.10.2023 – Organisation der Informationssicherheit in der Bundesagentur für Arbeit (BA)

Laufende Nummer: 202310005

Geschäftszeichen: IT2 – 1511 / 1500.3 / 1598 / 1680 / 1937 / 2223 / 2668 / 2665 / 123 / II-5214 / II-4011 /II-4302

Gültig ab: 01.11.2023

Gültig bis: unbegrenzt

SGB II: Information

SGB III: Weisung

Familienkasse: Weisung

Bezug:

- Leitlinie des Vorstandes zur Informationssicherheit

Aufhebung von Regelungen:

- HEGA 06/15 – 09 – Organisation der Informationssicherheit in der Bundesagentur für Arbeit (BA)

Zur Aufrechterhaltung und Erhöhung des Niveaus der Informationssicherheit in den BA-Geschäftsprozessen ist die Aufbau- und Ablauforganisation der Informationssicherheit in der BA festgelegt.

1. Ausgangssituation

Aktuelle Ereignisse zeigen, die Informationssicherheit der IT betrifft alle, sowohl Bürger/innen in einer Informationsgesellschaft als auch die Mitarbeitenden der BA im Umgang mit der Informationstechnologie (IT). Sozialdaten, die im Internet öffentlich zugänglich sind, personenbezogene Daten, mit denen gehandelt wird, und immer wieder auftretende Angriffsmeldungen zeugen von der Notwendigkeit einer handlungsfähigen Informationssicherheitsorganisation.



Die IT ist ein wichtiger Bestandteil für die erfolgreiche Aufgabenerledigung der BA. Dabei kommt der Informationssicherheit eine besondere Bedeutung zu. Sowohl Kundinnen und Kunden als auch Mitarbeitende der BA erwarten zu Recht, dass ihre Daten nur für den vorgesehenen Zweck verwendet werden und vor Missbrauch geschützt sind. Hierfür Sorge zu tragen, ist Aufgabe aller Führungskräfte und Mitarbeitenden der BA.

Die BA unterliegt gesetzlichen Rahmenbedingungen, unter anderem dem BSI-Gesetz, der KRITIS-Verordnung und den Planungsratsbeschlüssen. In diesen wurden zum Schutz der Informationsinfrastruktur der Bundesrepublik Deutschland - zu der auch die BA gehört - Maßnahmen der Informationssicherheit verbindlich festgelegt, die in der BA umgesetzt werden müssen bzw. deren Umsetzung nachgehalten werden muss.

Mit dem Vorstandsbeschluss 27/2006 wurde die Aufbau- und Ablauforganisation einer ganzheitlichen Informationssicherheitsorganisation in der BA beschlossen. Die Informationssicherheitsorganisation ist gemäß HEGA 06/15 – 09 mit einer Steuerungseinheit für Angelegenheiten der Informationssicherheit in der Zentrale, einer operativen Organisationseinheit im IT-Systemhaus und IT-Sicherheitsverantwortlichen (IT-SV) in den Dienststellen sowie im Regionalen Infrastrukturmanagement (RIM-IT-SV) der BA bzw. Organisationseinheiten nach SGB II (OE-SGB II) aufgebaut worden.

Mit dem Vorstandsbeschluss vom 68/2023 vom 16. Juni 2023 wurde die Gewährleistung der IT-Sicherheit in den Dienststellen neu systematisiert und deren geschäftspolitische Bedeutung für die Aufgabenerledigung gestärkt.

2. Auftrag und Ziel

Es ist sicherzustellen, dass nach Maßgabe der nachfolgenden Regelungen in folgenden Dienststellen bzw. Organisationseinheiten der BA IT-Sicherheitsverantwortliche eingesetzt sind. Dabei ist gemäß des Vorstandsbeschlusses unter bestimmten Voraussetzungen die Gewährung der Funktionsstufe für IT-SV vorgesehen.

2.1 Örtliche IT-Sicherheitsverantwortliche (IT-SV)

2.1.1 Aufgaben der IT-SV

Die IT-SV haben folgende Aufgaben:

- Durchführung einer jährlichen Informationssicherheitsüberprüfung mittels Checkliste.
- Erstellung von Halbjahresberichten über aufgetretene Informationssicherheitsvorfälle.

- Lfd. als Ansprechpartner/in zur Informationssicherheit für Mitarbeitende zur Verfügung stehen.
- Schulung von Führungskräften zur Sensibilisierung der dazugehörigen Mitarbeitenden. Die dafür notwendigen Mittel und Informationen werden von Seiten der zentralen Informationssicherheitsorganisation zur Verfügung gestellt.
- Verpflichtende Teilnahme an mindestens einer jährlichen Informationssicherheitsinformationsveranstaltung der zentralen Informationssicherheitsorganisation.
- Eigenständige Durchführung von mindestens einer jährlichen Lagebesprechung bezüglich der Informationssicherheit mit den Führungskräften der jeweiligen Dienststellen/ Organisationseinheiten.
- Erste/r Ansprechpartner/in bei Fragen der Mitarbeitenden bei der Durchführung der verpflichtenden Teilnahme der Selbstlernmedien der BA-Lernwelt (nachfolgend als „Web Based Trainings“ (WBT) bezeichnet) zur Informationssicherheit.
- Nachhaltung der Vorgaben der Informationssicherheit und das Auditieren der Mitarbeitenden mittels Checkliste.
- Informationen zu Informationssicherheitsvorfällen der Mitarbeitenden werden an die zuständigen Stellen weitergegeben.

Ein/e IT-SV hat die folgenden Anforderungen zu erfüllen:

- Grundkenntnisse der Methodik und Didaktik,
- Grundkenntnisse zur Steuerungslogik der BA,
- Anwenderkenntnisse der maßgeblichen IT-Fachverfahren für die Anwendergruppe,
- Grundkenntnisse IT-spezifischer Hintergründe der IT-Fachverfahren für die Anwendergruppe sowie ggf. von Schnittstellen zu angrenzenden IT-Systemen im erforderlichen Rahmen.

Die Anforderungen werden in der Regel von Beschäftigten erfüllt, die auf Tätigkeiten der TE IV angesetzt sind und über eine gewisse IT-Affinität verfügen. Es können auch geeignete Beschäftigte mit entsprechender IT-Affinität in Betracht kommen, die auf Tätigkeiten der TE V angesetzt sind.

2.1.2 Auswahl der IT-SV

Die Auswahl und Festlegung der Anzahl der notwendigen örtlichen IT-SV erfolgt unter Berücksichtigung der Dienststellenstruktur und der Aufwandsaspekte durch die örtliche Geschäftsführung, d.h.:

- für Agenturen für Arbeit (AA) durch den/die VG,
- für die gemeinsamen Einrichtungen/Jobcenter durch den/die Geschäftsführer/in,
- für die RD durch den/die VG der RD,
- für die FamKa Direktion durch den/die Leiter/in,
- für die ZAV durch den/die VG,
- für das IAB durch den/die Leiter/in,
- für das BA-Service-Haus durch den/die VG,
- für die Führungsakademie durch der/die Geschäftsführer/in,
- für die Hochschule durch den/die Kanzler/in,
- für das IT-Systemhaus durch den/die VG,
- für die Zentrale durch den/die Informationssicherheitsbeauftragte/n der BA

Nach Auswahl der örtlichen IT-SV sind die Mitarbeitenden der jeweiligen Dienststellen und der örtlich zuständige RIM zu informieren. Entsprechende Berechtigungen sind durch den/die IT-SV zu bestellen bzw. abzubestellen.

Als Richtwert für die Anzahl der zu benennenden IT-SV im Verantwortungsbereich müssen die Schwellenwerte (siehe Pkt. 3.1) als Grundlage herangezogen werden.

Eine gleichzeitige Wahrnehmung der Funktion des/der Ansprechpartner/in Datenschutz und des/der IT-Sicherheitsverantwortlichen ist nicht zu empfehlen.

2.1.3 Zeitlicher Aufwand für Aufgaben der IT-SV

Maßstabsdienststelle für die Aufwandsermittlung ist eine Dienststelle mit 700 Mitarbeitenden. Der durchschnittliche Monatsaufwand für eine Maßstabsdienststelle beläuft sich auf ca. 12 Stunden (Zu-/ Abschläge entsprechend der tatsächlichen Zahl der Mitarbeitenden).

2.1.4 Einweisungs- und Informationsangebot

Die Einweisung in die IT-SV Aufgaben erfolgt durch den/die zuständige/n RIM-IT-SV entsprechend den örtlichen Gegebenheiten. Für die Einweisung ist ein Arbeitstag einzuplanen. Die IT-SV informieren sich über aktuelle informationssicherheitsrelevante Angelegenheiten und Sensibilisierungsthemen auf der Seite der Informationssicherheit im BA-Intranet.

Die zentrale Informationssicherheitsorganisation führt mindestens eine jährliche Informationsveranstaltung für die IT-SV durch und unterstützt neue IT-SV beim Onboarding-Prozess.

Die IT-SV informieren die Führungskräfte über die Verfügbarkeit von Schulungsmaterialien.

Im Übrigen müssen sich die IT-SV eigenständig fortbilden, indem sie aktuelle Geschehnisse im Fokus haben. Hierfür sind die einschlägig bekannten Informationsquellen zu nutzen (z.B. Informationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Meldungen vom CERT-Bund etc.).

2.2 Berichtswesen

Die Berichtsinhalte und die Aufbewahrungszeit sind den Hinweisen zu entnehmen.

2.2.1 Berichtstermine IT-SV

Die Informationssicherheitsberichte sind halbjährlich und die Checkliste einmal im Jahr zu erstellen. Es gelten folgende Termine zur Meldung an den jeweiligen RIM-IT-SV

- 14.07. des lfd. Jahres: Abgabe des Halbjahresberichts für den Zeitraum 01.01. - 30.06.
- 19.01. des Folgejahres: Abgabe des Halbjahresberichts für den Zeitraum 01.07. - 31.12. und der bearbeiteten Checklisten für den Zeitraum 01.01. - 31.12.

2.2.2 Berichtstermine RIM-IT-SV

Die Informationssicherheitsberichte für den RIM-IT-SV-Bezirk sind halbjährlich und die Checkliste einmal im Jahr zu erstellen. Für die RIM-IT-SV gelten folgende Termine zur Meldung an die RIM-Steuerung im BA-SH:

- 31.07. des lfd. Jahres: Abgabe des Halbjahresberichts für den Zeitraum 01.01. - 30.06.
- 31.01. des Folgejahres: Abgabe des Halbjahresberichts für den Zeitraum 01.07. - 31.12. und der bearbeiteten Checklisten für den Zeitraum 01.01. - 31.12.

2.2.3 Berichtstermine RIM-Steuerung

Der zusammenfassende Informationssicherheitsbericht für alle RIM-IT-SV-Bezirke ist halbjährlich und die Zusammenfassung der Checklisten der IT-SV und RIM-IT-SV einmal im Jahr zu erstellen. Für die RIM-Steuerung gelten folgende Termine zur Meldung an IT2:

- 31.08. des lfd. Jahres: Abgabe des Halbjahresberichts für den Zeitraum 01.01. - 30.06.
- 28.02. des Folgejahres: Abgabe des Halbjahresberichts für den Zeitraum 01.07. - 31.12. und der bearbeiteten Checklisten für den Zeitraum 01.01. - 31.12.

2.3 Der Sensibilisierungsprozess für Informationssicherheit

Die durch den Vorstand unterzeichnete Leitlinie zur Informationssicherheit gilt verbindlich für alle Mitarbeitenden der BA.

Auf der Seite der Informationssicherheit im BA-Intranet stehen Informationen zur Sensibilisierung zur Verfügung. Mit Hilfe barrierefreier webbasierter Trainings (WBT) werden IT-Anwender/Innen auch ohne besondere IT-Kenntnisse über richtige Verhaltensweisen im Sinne der Informationssicherheit informiert und sensibilisiert.

2.4 Durcharbeitung der WBT der Informationssicherheit

Die BA unterliegt als Betreiberin einer Kritischen Infrastruktur den gesetzlichen Anforderungen des BSI-Gesetzes (BSIG). Nach den Vorgaben des BSIG müssen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen betreffend der betriebenen Kritischen Infrastruktur getroffen werden. Hieraus leitet sich eine Empfehlung für eine jährlich wiederkehrende Durcharbeitung der WBT zu ausgewählten Themen der Informationssicherheit ab.

Die lokale Dienststellenleitung ist verantwortlich dafür, dass im dazugehörigen Zuständigkeitsbereich alle Mitarbeitenden die WBT absolvieren können. Bei neu eingestellten Mitarbeitenden ist dies bereits im Rahmen der Einarbeitungsprogramme verpflichtend vorzusehen. Danach wird empfohlen, die Durcharbeitung einer Auswahl der WBT jährlich zu wiederholen. Darüber hinaus haben alle Mitarbeitenden die Möglichkeit, Teile der WBT beliebig oft zu wiederholen. Die Nachhaltung der Durcharbeitung der WBT liegt im Verantwortungsbereich des/der Mitarbeitenden und wird durch IT-SV im Rahmen der jährlichen Mitarbeitenden-Unterweisung nachgehalten.

2.5. Verpflichtung zur jährlichen Sensibilisierung

Führungskräfte sind jährlich dazu verpflichtet, ihre Mitarbeitenden im Themengebiet der Informationssicherheit zu sensibilisieren. Die Materialien zur Sensibilisierung werden von der zentralen Informationssicherheitsorganisation bereitgestellt und durch die (RIM-) IT-SV an die zuständigen Führungskräfte verteilt.

2.6 Zahlung einer Funktionsstufe

Mitarbeitende, die als IT-SV beauftragt werden, erhalten grundsätzlich eine der Bedeutung dieser Aufgabe entsprechende tätigkeitsunabhängige Funktionsstufe 1. Die Höhe des Funktionsstufenbetrages richtet sich nach der Tätigkeitsebene, der der originär übertragene Dienstposten zugeordnet ist.

Erfolgt die Beauftragung von Mitarbeitenden der Tätigkeitsebene V, richtet sich die Höhe des Funktionsstufenbetrages nach der Tätigkeitsebene IV.

Die Zahlung erfolgt im Vorgriff auf die zu gegebener Zeit beabsichtigte Tarifierung zunächst übertariflich. Mit Wirkung vom Inkrafttreten der Tarifierung wird eine auf Grundlage dieser Weisung übertariflich gewährte Funktionsstufe durch die für diesen Anlass tarifierte Funktionsstufe ersetzt, sofern die sonstigen Voraussetzungen weiterhin vorliegen. Unbeschadet dessen finden die für tätigkeitsunabhängige Funktionsstufen geltenden tariflichen Regelungen entsprechend Anwendung.

Von der Zahlung dieser Funktionsstufe ausgenommen sind Mitarbeitende, denen Dienstposten oder Rollen bzw. Funktionen übertragen sind, bei denen die Gewährleistung der Informationssicherheit Teil der dienstlichen Tätigkeit ist oder die im Rahmen der mit ihrer Tätigkeit verbundenen Vorbildfunktion bzw. den mit ihrer Tätigkeit verbundenen Aufgaben dazu beitragen, ein angemessenes Informationssicherheitsniveau zu gewährleisten. In diesen Fällen sind Verantwortlichkeiten und Handlungserfordernisse im Kontext der Informationssicherheit als dienstpostenimmanent zu betrachten. Hierunter fallen die Aufgabenträger/innen im IT-Systemhaus sowie in den IT-Services der RIM (RIM-IT-SV) sowie IT-Fachbetreuer/innen.

3. Einzelaufträge

3.1 Die Geschäftsführung bzw. Leitung vor Ort in allen Dienststellen

- trifft die Auswahl der Mitarbeitenden und legt die Anzahl der IT-SV anhand der festgelegten Schwellenwerte fest. Dabei ist unter Beachtung der Wirtschaftlichkeit, Wirksamkeit und des aufgebauten Know-hows, mindestens ein/e IT-SV zu benennen.

Folgende Schwellenwerte sind für die Benennung von „hauptverantwortlichen“ IT-SV zu berücksichtigen:

- Mitarbeitendenanzahl ab 200 bis 699 einen IT-SV
 - Mitarbeitendenanzahl ab 700 bis 1199 zwei IT-SV
 - Mitarbeitendenanzahl ab 1200 bis 1699 drei IT-SV
 - Mitarbeitendenanzahl ab 1700 bis 2199 vier IT-SV
 - Mitarbeitendenanzahl ab 2200 fünf IT-SV
- In allen Dienststellen mit einer Mitarbeitendenanzahl unter 200 werden aufgrund des geringeren Aufwands ausschließlich vorhandene IT-Fachbetreuer/innen als IT-SV beauftragt. Eine zusätzliche Funktionsstufe wird nicht gewährt.
 - stellt sicher, dass mindestens ein/e Mitarbeitende/r je Dienststelle benannt ist und die erforderliche Entlastung von den originär wahrzunehmenden Aufgaben zur angemessenen Ausübung der Funktion erfolgt.
 - weist auf die Verpflichtung zur Durcharbeitung der WBT hin.
 - hält die Durcharbeitung der WBT nach und regelt die Dokumentation in eigener Verantwortung.
 - stellt über den IM-Webshop den Zugriff auf die Austauschablage der IT-SV sicher.
 - wirken darauf hin, dass in gemeinsamen Einrichtungen entsprechend der vorstehenden Regelungen IT-SV beauftragt werden. Der Anspruch auf die (über-)tarifliche Zulage von Funktionsstufen an BA-Beschäftigte in den gemeinsamen Einrichtungen richtet sich nach den vorstehenden Regelungen.

3.2 Der/Die RIM-IT-SV

- weist die neuen IT-SV einmalig ein.
- verteilt die Unterlagen an die IT-SV.
- erstellt die Halbjahresberichte (siehe Punkt 2.2.2) und sendet diese an die RIM-Steuerung.

3.3 Die RIM-Steuerung

- verteilt die Unterlagen an die RIM-IT-SV.

- erstellt die Halbjahresberichte (siehe Punkt 2.2.3) und sendet diese an IT2.

3.4 Der/Die örtliche IT-SV

- prüft stichprobenartig die Absolvierung der jährlichen WBT im Rahmen der jährlichen Mitarbeitenden-Unterweisung.

3.5 Die Internen Services Personal

- begleiten den Auswahlprozess für die IT-SV.
- stellen bei Erfüllung der Voraussetzungen die Zahlung der Funktionsstufe sicher.
- überwachen die übertarifliche Zahlung im Hinblick auf die zu einem späteren Zeitpunkt beabsichtigte Tarifierung

4. Info

Entfällt

5. Haushalt

Einbringung der benötigten Haushaltsmittel für die Gewährung der Funktionsstufe für IT-SV.

6. Beteiligung

Der Hauptpersonalrat und die Hauptschwerbehindertenvertretung wurden beteiligt.