Weisung 202407005 vom 11.07.2024 – Organisation der Informationssicherheit in der Bundesagentur für Arbeit (BA)

Laufende Nummer: 202407005

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

Gültig ab: 11.07.2024
Gültig bis: unbegrenzt

SGB II: Information
SGB III: Weisung
Familienkasse: Weisung

Bezug:

- Leitlinie des Vorstandes zur Informationssicherheit

Aufhebung von Regelungen:

- Weisung 202310005 vom 20.10.2023 – 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 Bürgerinnen und Bürger 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.

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 Weisung 202310005 vom 20.10.2023 – Organisation der Informationssicherheit in der Bundesagentur für Arbeit (BA) wurden zur Aufrechterhaltung bzw. Erhöhung der Informationssicherheit in den BA-Geschäftsprozessen die Aufbau- und Ablauforganisation der Informationssicherheit in der BA neu festgelegt. Bestandteil waren u.a. Regelungen zu den örtlichen IT-Sicherheitsverantwortlichen, deren Aufgaben und Verteilung. Mit der vorliegenden Weisung werden diese Regelungen weiter geschärft sowie die Verteilung neu geregelt.

Das Betreuungskonzept sah bisher vor, dass in kleineren Dienststellen unter 200 Beschäftigten aus dem Kreis vorhandener IT-Fachbetreuerinnen und Fachbetreuer eine Person die Funktion der IT-SV mit übernimmt. In diesen Fällen war die Zahlung einer weiteren Funktionsstufe für die IT-SV ausgeschlossen, weil die Anforderungen mit der für die IT-Fachbetreuung bereits gezahlten Funktionsstufe als abgegolten betrachtet werden sollten. In größeren Dienststellen (ab 200 Beschäftigten) sollte die IT-SV als eigenständige Funktion übertragen werden. Ab 700 Beschäftigte konnte ein/e zweite IT-SV bestellt werden. Weitere IT-SV konnten je 500 weitere Beschäftigte hinzukommen.

Um tarifvertraglich eine für die IT-SV beabsichtigte Funktionsstufenzahlung vereinbaren zu können, musste im Ergebnis der Tarifverhandlungen das Betreuungskonzept nochmal modifiziert werden.

2. Auftrag und Ziel

Es wird ein geändertes Betreuungskonzept implementiert. Die Voraussetzungen zur Auswahl und Übertragung der IT-SV und die Schwellenwerte für die Anzahl von IT-SV haben sich geändert. Insbesondere der bisherige Schwellenwert „200“ entfällt, da die IT-SV mit Inkrafttreten dieser Weisung stets eine eigenständige, für sich alleinstehende Funktion ist. Darüber hinaus ist künftig ein einheitliches, in Teilen größeres Raster in den Betreuungsumfängen vorgesehen. Die vorherige Kombination mit der IT-Fachbetreuung ist generell nicht mehr zulässig.

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

Die Umsetzung erfolgt einheitlich ab dem 01.09.2024.

2.1 Örtliche (RIM-) IT-Sicherheitsverantwortliche

2.1.1 Aufgaben der RIM-IT-SV

Die RIM-IT-SV

Die RIM-IT-SV haben folgende Aufgaben:

- Ansprechperson für das Erstellen der Halbjahresberichte der IT-SV.
- Konsolidierung der Halbjahresberichte der IT-SV und Ableitung der Handlungsbedarfe.
- Einweisung neuer IT-SV und ggf. Wissensauffrischung (kann durch RIM-IT-SV an geeignetes RIM-Personal delegiert werden).
- Kommunikation zu informationssicherheitsbezogenen Themen im eigenen RIM-Bezirk.
- Ansprechperson für allgemeine informationssicherheitsbezogene Belange der IT-SV und des RIM, beispielsweise als erste Eskalationsinstanz.
- Sicherstellung der RIM Geschäftsprozesse zur Informationssicherheit.
- Auditieren der Richtlinien zur Informationssicherheit mittels Template (kann durch RIM-IT-SV an geeignetes RIM-Personal delegiert werden).

- Nachhalten der eigenständigen Durchführung von mindestens einer Besprechung zu aktuellen Themen der Informationssicherheit durch IT-SV.
- Nachhalten der jährlichen Sensibilisierung der Führungskräfte durch IT-SV.
- Nachhalten der Teilnahme von IT-SV an mindestens einer jährlichen Großkonferenz.

2.1.2 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 Besprechung zu aktuellen Themen 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.

2.1.3 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.

In jeder Dienststelle wird grundsätzlich (wie bisher) ein/e IT-SV bestellt. Als Richtwert für die Benennung weiterer IT-SV im Verantwortungsbereich müssen die neuen Schwellenwerte (siehe Pkt. 3.1) als Grundlage herangezogen werden.

Die Rolle der IT-SV ist nunmehr stets eine für sich alleinstehende Funktion.

Um den Anforderungen als IT-SV im gebotenen Maße gerecht werden zu können, ist daher eine Kombination mit anderen Rollen bzw. Funktionen, für die tätigkeitsunabhängige Funktionsstufen gewährt werden können, insbesondere mit anderen tätigkeitsunabhängigen IT-Funktionen (IT-Fachbetreuung/ web-Autor/-in) untersagt.

Weiterhin muss die Wahrnehmung der Rolle IT-SV mit der originär übertragenen Tätigkeit vereinbar sein.

2.1.4 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).

2.1.5 Einweisungs- und Informationsangebot

Die Einweisung in die IT-SV Aufgaben erfolgt grundsätzlich durch den/die zuständige/n RIM-IT-SV entsprechend den örtlichen Gegebenheiten und unter Berücksichtigung der verfügbaren Ressourcen. Für die Einweisung ist ein Arbeitstag einzuplanen und ist durch die IT-SV zeitnah nach der Benennung verpflichtend wahrzunehmen.

Für Mitarbeitende die bereits als IT-SV tätig waren und in der Vergangenheit entsprechend unterwiesen wurden, ist eine erneute Unterweisung nicht zwingend erforderlich. Sofern die letzte Unterweisung vor Inkrafttreten der vorherigen Weisung erfolgte, soll jedoch den betroffenen IT-SV ein optionales Angebot zur Auffrischung der Kenntnisse gemacht werden.

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.).

Die RIM IT-SV stehen im Übrigen für Rückfragen zur Verfügung und bieten bedarfsabhängig kurze Auffrischungen der erfolgten Unterweisungen an.

2.2 Berichtswesen

Die Berichtsinhalte und die Aufbewahrungszeit sind den Hinweisen(DOCX DOCX, Stand 24.07.2023) 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 die zentrale Informationssicherheitsorganisation:

- 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

Tarifbeschäftigte, die als IT-SV beauftragt werden, erhalten eine der Bedeutung dieser Aufgabe entsprechende tätigkeitsunabhängige Funktionsstufe 1. Die Höhe des Funktionsstufenbetrages richtet sich nach grundsätzlich 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, in den IT-Services der RIM (RIM-IT-SV) und Mitarbeitende des Informations-Sicherheitsmanagements (ISM).

3. Einzelaufträge

3.1 Die Geschäftsführung bzw. Leitung vor Ort in allen Dienststellen

- überprüft die bisherigen Festlegungen zur Auswahl und Anzahl von IT-SV mit Blick auf die geänderten Schwellenwerte, trifft die Auswahl der Mitarbeitenden und legt die Anzahl der IT-SV anhand der neuen Schwellenwerte fest. Dabei ist unter Beachtung der Wirtschaftlichkeit, Wirksamkeit und des aufgebauten Know-hows, mindestens ein/e IT-SV je Dienststelle zu benennen.

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

- Mitarbeitendenanzahl bis 699 eine/n IT-SV
- Mitarbeitendenanzahl ab 700 bis 1399 zwei IT-SV

- Mitarbeitendenanzahl ab 1400 bis 2099 drei IT-SV
- Mitarbeitendenanzahl ab 2100 vier IT-SV
- 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 sowie die Erfordernis der jährlichen Sensibilisierung der Führungskräfte durch die IT-SV hin.
- regelt die Nachhaltung und Dokumentation der Durcharbeitung der WBT in eigener Verantwortung.
- stellt über den IM-Webshop den Zugriff auf die Austauschablage der IT-SV sicher.
- wirkt darauf hin, dass in den zugeordneten gemeinsamen Einrichtungen entsprechend der vorstehenden Regelungen IT-SV beauftragt werden. In diesem Fall richtet sich der Anspruch auf die (über-)tarifliche Zahlung von Funktionsstufen an BA-Beschäftigte in den gemeinsamen Einrichtungen nach den vorstehenden Regelungen.

3.2 Der/Die RIM-IT-SV

- sorgt für die erstmalige Einweisung der neuen IT-SV.
- verteilt die Unterlagen an die IT-SV und je nach örtlichen Gegebenheiten für die jährliche Sensibilisierung an die Führungskräfte
- 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 die zentrale Informationssicherheitsorganisation.

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 und administrieren die erforderlichen Geschäftsverteilungen.
- prüfen, dass die Auswahl und Anzahl der IT-SV den Vorgaben der Weisung entspricht und widerrufen ggf. die nicht den nunmehr geltenden Regelungen entsprechenden Übertragungen.
- 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

Die benötigten Haushaltsmittel für die Gewährung der Funktionsstufe für die IT-SV werden zentral im Haushalt berücksichtigt.

6. Beteiligung

Der Hauptpersonalrat und die Hauptschwerbehindertenvertretung wurden beteiligt.

gez.
Unterschrift