|  |
| --- |
| **Vorlage** |
| **Erweiterte ISDS Dokumentation für Vertragspartner von IT-Stellen** |
| Bundesamt für Sozialversicherungen |
| 14.10.2024 |

Dokumentinformationen

|  |  |  |
| --- | --- | --- |
| Titel: | Erweiterte ISDS Dokumentation für Vertragspartner von IT-Stellen | |
| Veröffentlichungsdatum: | 14.10.2024 | |
| Gespeichert: | 14. Oktober 2024 | |
| Anzahl Seiten: | 13 | |
| Dateiname: | ISDS-Vorlage - Erweiterter Schutz\_Dritte.docx | |
| Dokumentverantwortlicher: | BSV, DS-ITM | |
| Status: | Entwurf | |
| Geprüft durch: | BSV, | Datum: 31.12.2024 |

Versionen

| Version des Dokuments | Datum | Wichtigste Änderungen | Verantwortlich |
| --- | --- | --- | --- |
| V0.1 | 14.10.2024 | Erstellung | M. Burri  M. Moog |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Abkürzungen und Begriffe

|  |  |
| --- | --- |
| Abkürzung | Beschreibung |
| AK | Ausgleichskasse |
| DS | Durchführungsstelle |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Referenzierte Dokumente

Gewisse sicherheitsrelevante Aspekte sind in separaten Dokumenten festgehalten. Auf die folgenden Dokumente wird im Rahmen dieses ISDS-Konzepts referenziert:

| Titel | Autor / Herausgeber | Datum |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Inhaltsverzeichnis

[1. Zweck des Dokuments 5](#_Toc180159963)

[2. Management Summary 5](#_Toc180159964)

[2.1. Allgemeines 5](#_Toc180159965)

[2.2. Zusammenfassung Restrisiken 5](#_Toc180159966)

[2.3. Abschliessende Bemerkungen 5](#_Toc180159967)

[3. Verzeichnis der sicherheitsrelevanten Dokumente 5](#_Toc180159968)

[4. Einstufung an Hand Schutzbedarfsanalyse 6](#_Toc180159969)

[5. Sicherheitsrelevante Systembeschreibung 7](#_Toc180159970)

[5.1. Ansprechpartner und Verantwortlichkeiten 7](#_Toc180159971)

[5.2. Beschreibung des Gesamtsystems/Vertragsobjekt 7](#_Toc180159972)

[5.3. Beschreibung der zu bearbeitenden Daten 7](#_Toc180159973)

[5.4. Architekturskizze & Kommunikationsmatrix 8](#_Toc180159974)

[5.5. Beschreibung der zugrundeliegenden Technik 9](#_Toc180159975)

[6. Risikoanalyse und Schutzmassnahmen 10](#_Toc180159976)

[6.1. Restrisiken 10](#_Toc180159977)

[6.1.1. Erhöhte Restrisiken (rot) 11](#_Toc180159978)

[6.1.2. Erhöhte Restrisiken (gelb) 11](#_Toc180159979)

[6.2. Besonders zu beachtende Punkte 12](#_Toc180159980)

[7. Wiederherstellung des Geschäftsbetriebes 12](#_Toc180159981)

[8. Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen 12](#_Toc180159982)

[8.1. Systemabnahmeprüfung 12](#_Toc180159983)

[9. Ausserbetriebnahme 12](#_Toc180159984)

[10. Abkürzungen 13](#_Toc180159985)

[11. Anhang 13](#_Toc180159986)

# Zweck des Dokuments

Das ISDS-Konzept legt die nötigen Angaben zur Erhaltung und Verbesserung der Informationssicherheit und des Datenschutzes fest. Es fasst die Aspekte der Informationssicherheit und des Datenschutzes de entsprechenden IT-Systeme oder Services zusammen und beschreibt das IT-System als Ganzes, dokumentiert die Risikoanalyse sowie die getroffenen Schutzmassnahmen.

# Management Summary

Das Management-Summary fasst den Zweck des Vertragsgegenstandes, die Ergebnisse aus der Schutzbedarfsanalyse sowie die getroffenen Massnahmen kurz zusammen. Es sollte so geschrieben sein, dass es auch für technisch nicht-versierte Menschen gut verständlich ist. Das Management-Summary fasst zudem die verbliebenen Restrisiken zusammen, die durch mit der Abnahme des vorliegenden ISDS-Konzepts durch die Geschäftsleitung getragen werden.

Es wird empfohlen, das Management-Summary am Schluss der Erstellung (nach dem ersten Review) zu verfassen

## Allgemeines

Zusammenfassung der Angaben im Dokument über die getätigte Risikoanalyse, die Informationssicherheit und den Datenschutz. Zeigt ein Bild über das vorhandene Risikopotential des untersuchten Systems auf.

## Zusammenfassung Restrisiken

Aus dem Kapitel 6.1 ist die Zusammenfassung und Beurteilung der Restrisiken zu erstellen. Der Entscheid darüber, ob die Restrisiken in Kauf genommen werden, obliegt den Vertragspartnern.

## Abschliessende Bemerkungen

Abschliessende wichtige Bemerkungen und Fazits zum vorliegenden Vertragsobjekt.

# Verzeichnis der sicherheitsrelevanten Dokumente

Hier sind die rechtlichen Grundlagen anzuführen auf die sich das (zu realisierende) IT-Vorhaben abstützt. Neben behördlichen Vorgaben (Gesetzen, Verordnungen, Weisungen) sind auch interne Dokumente aufzuführen.

Risiken und Gefahren können teilweise durch übergeordnete Sicherheitskonzepte oder SLA abgedeckt sein. Diese Dokumente sind hier aufzuführen.

|  |  |
| --- | --- |
| Dokumententyp | Titel |
| Gesetz | [SR 235.1 Bundesgesetz über den Datenschutz (DSG)](http://www.admin.ch/ch/d/sr/c235_1.html) |
|  | [SR 152.1 Bundesgesetz über die Archivierung (Archivierungsgesetz, BGA)](http://www.admin.ch/ch/d/sr/c152_1.html) |
|  |  |
| Verordnung | [AS 2022 568 - Datenschutzverordnung](https://www.fedlex.admin.ch/eli/oc/2022/568/de) |
|  | [SR 235.11 Verordnung zum Bundesgesetz über den Datenschutz (VDSG)](http://www.admin.ch/ch/d/sr/c235_11.html) |
|  | [SR 172.010.58 Verordnung](https://www.fedlex.admin.ch/eli/cc/2020/988/de)  [über die Koordination der digitalen Transformation](https://www.fedlex.admin.ch/eli/cc/2020/988/de)  [und die IKT-Lenkung in der Bundesverwaltung (VDTI)](https://www.fedlex.admin.ch/eli/cc/2020/988/de) |
|  | [SR 172.010.442 Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen](http://www.admin.ch/ch/d/sr/c172_010_442.html) |
|  |  |
| Weisung | Weisungen des BSV (W-ISDS, weitere) |
|  |  |
| Strategie |  |
|  |  |
|  |  |
| Übergeordnete Sicherheitskonzepte |  |
| SLA |  |
| Weitere interne Dokumente | 🡺 Vom Verfasser zu ergänzen |

# Einstufung an Hand Schutzbedarfsanalyse

Die Einstufung des Vertragsobjektes/Services muss gemäss Schutzbedarfsanalyse (Schuban), vorgenommen werden.

Mit den Beurteilungen in der Schuban sollen auch allfällige finanzielle Folgen von Sicherheitsbedürfnissen geschätzt und im Dokument beschrieben werden.

Die Zusammenfassung sowie die Einstufung der Schuban soll hier in Tabellenform dargestellt werden.

|  |  |
| --- | --- |
| **Ergebnis der Einstufung** | |
| **Vertraulichkeit:** | Werden Personendaten bearbeitet ? Wenn ja, besteht ein hohes Risiko ? |
| Klassierung gemäss internen Richtlinien, z. B. intern, vertraulich, … |
| Anforderungen an Vertraulichkeit (erhöht/nicht erhöht) |
| **Verfügbarkeit:** | Maximal zulässige Ausfalldauer, z. B. <2 Std, <8 Std, <12 Std, mehr als 12 Std |
| Maximal zulässiger Datenverlust, z. B. 30 Min, 2 Std, 24 Std |
| Notwendigkeit von IT Service Continuity Management (ITSCM) als Teil des Business Continuity Managements |
| **Integrität:** | Bestehen spezielle Anforderungen an die Integrität ? |
| **Nachvollziehbarkeit:** | Bestehen spezielle Anforderungen an die Nachvollziehbarkeit ? |

Erkenntnis aus der Schuban Normaler oder erhöhter Schutzbedarf

# Sicherheitsrelevante Systembeschreibung

Verdichtete Beschreibung der sicherheitsrelevanten Elemente aus dem System, den Anwendungen, den vorhandenen und bearbeiteten Datensammlungen und den dazugehörenden Prozessen.

## Ansprechpartner und Verantwortlichkeiten

|  |  |
| --- | --- |
| Wer | Name |
| Ansprechpartner IV Stelle |  |
| Ansprechpartner beim Vertragspartner |  |
| ISBD Vertragspartner |  |
| ISBO IV Stelle |  |
| weitere Stellen |  |

## Beschreibung des Gesamtsystems/Vertragsobjekt

Beschreibung des Systems als Ganzes sowie der sicherheitsrelevanten Funktionalitäten wie Rollenkonzepte, Authentisierungsmethode, Backup, Support- und Wartungsprozesse (evtl. Fernwartung), SLA etc.  
Es können auch Verweise auf entsprechende Dokumente (Name, Erstellungsdatum, Speicherort, etc.) gemacht werden. Die Beschreibung soll so ausgeführt sein, dass er vollständig und auch für Unbeteiligte verständlich und nachvollziehbar formuliert ist.

## Beschreibung der zu bearbeitenden Daten

Beschreibung der Daten und Strukturen (z.B. verwendete Datenbank).

Folgende Fragen müssen bei der Bearbeitung von Personendaten geklärt bzw. sollen beschrieben sein:

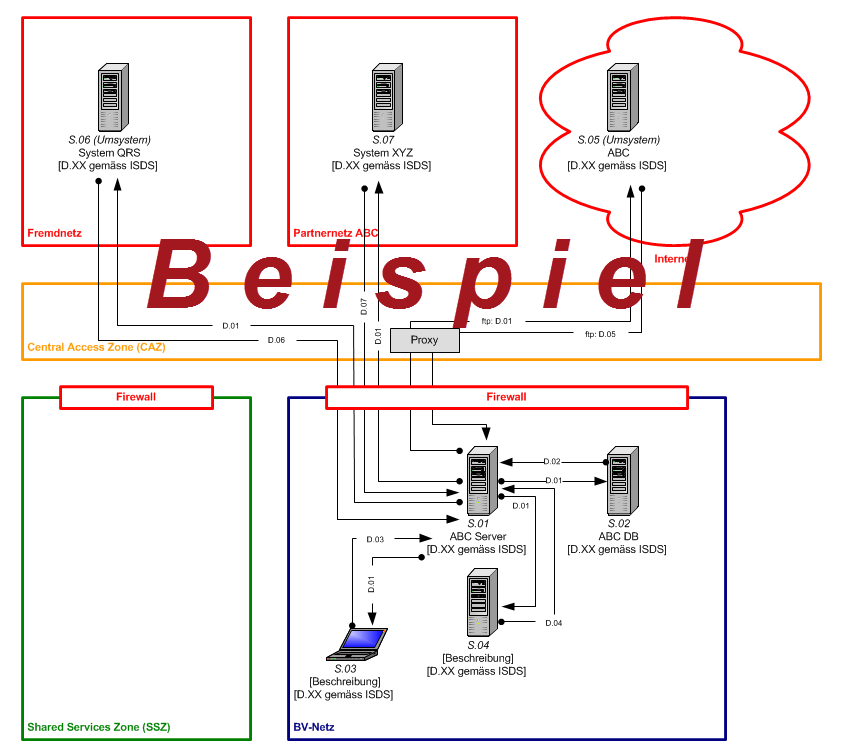
* Ist die Datensammlung beim EDÖB angemeldet?

Bei diesem Punkt geht es darum, festzustellen ob die Datenbearbeitung den Vorgaben des Datenschutzgesetztes genügt. Insbesondere ist zu prüfen ob eine Datensammlung beim EDÖB angemeldet werden muss oder nicht.

* Ist ein Bearbeitungsreglement zu erstellen?   
  Hilfe dazu finden Sie im Template [Bearbeitungsreglement](https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/prozesse-methoden/p042-informationssicherheits-und-datenschutzkonzept_ISDS.html) sowie in der Verordnung zum DSG und unter dem Link [Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes](https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html)  
  Wenn ja, Verweis zum entsprechenden Dokument.
* Besteht eine gesetzliche Grundlage zur elektronischen Bearbeitung der Daten?
* Müssen die Daten dem Bundesarchiv elektronisch zur Verfügung gestellt werden?
* Bei klassifizierten Informationen sind die ISchV & die detaillierten [Bearbeitungsvorschriften](https://intranet.vbs.admin.ch/de/wissen/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb.detail.document.html/vbs-intranet/de/documents/integrale-sicherheit/grundlagen-vorgaben-internationales/kischb/Bearbeitungsweisungend.pdf.html) (nur im Intranet verfügbar) zu beachten

## Architekturskizze & Kommunikationsmatrix

Hier eine Architekturskizze und eine Kommunikationsmatrix einfügen oder auf das entsprechende aktuell gehaltene Dokument verweisen.





## Beschreibung der zugrundeliegenden Technik

Beschreibung der verwendeten Techniken wie Serverplattform, Betriebssystem(e), Systemumfeld, verwendete Netzwerke, Kryptographische Funktionen etc. Sie sollen so beschrieben sein, dass es vollständig ist und auch für Unbeteiligte verständlich und nachvollziehbar.

Alternativ kann auf das entsprechende aktuell gehaltene Dokument verwiesen werden.

# Risikoanalyse und Schutzmassnahmen

Beschreibung der relevanten Risikofaktoren (Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit), Auflistung und Bewertung der Risiken, inkl. der Risiken.

Die detaillierte [Risikoanalyse](https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren/erhoehter-schutz.html) ist anhand der zum Konzept/zur DSFA gehörenden Excel-Datei vorzunehmen. Hinweise zum Ausfüllen sind im Excel-Dokument zu finden.

Ergebnisse aus der Risikoanalyse:

In der Arbeitsmappe «Restrisikomatrix» ist beschrieben, in welcher Kategorie sich das beurteilte Restrisiko befindet.

Grün: sind Risiken die entweder inhärent (im Service als solche) sind oder aber vernachlässigt werden können. Sollen mit einfachen Massnahmen minimiert werden können.

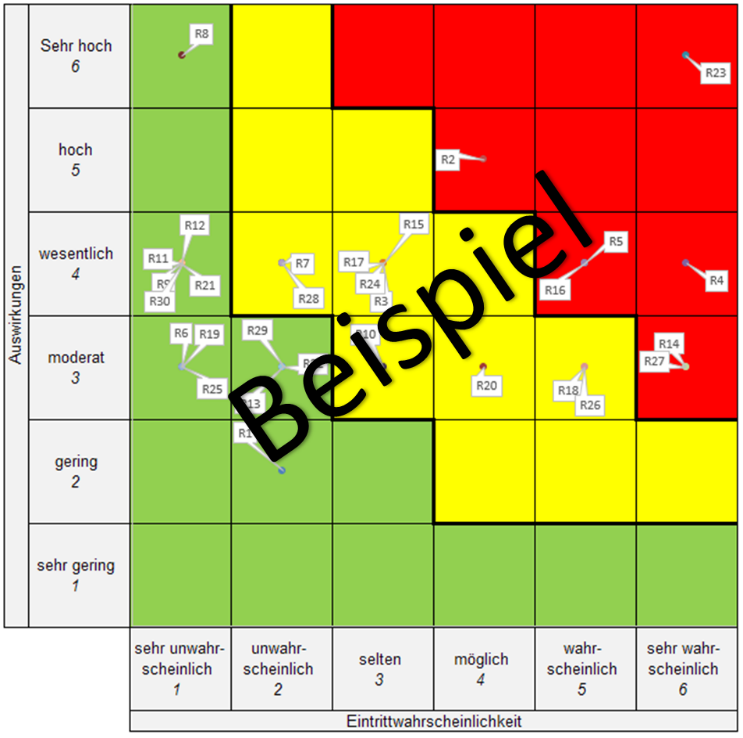
Gelb: Risiken deren Auswirkungen erheblich sind und deshalb reduziert werden müssen.

Rot: Grosse Risiken deren Auswirkungen kritisch bis katastrophal sind. Diese Risiken müssen unbedingt reduziert werden.

🡺 Risiken die nicht oder ungenügend reduziert werden (aus der Restrisikomatrix rot oder gelb markiert), müssen im ISDS-Konzept (Kapitel 6.1) ausgewiesen werden. Sie sind auszuweisen und dem Auftraggeber und dem Geschäftsprozessverantwortlichen schriftlich zur Kenntnis zu bringen. Der Entscheid darüber, ob bekannte Restrisiken in Kauf genommen werden, obliegt dem Leiter der zuständigen Verwaltungseinheit.   
  
Die Restrisiken müssen auch im Management-Summary (Kapitel 2.2) kurz zusammengefasst werden.

## Restrisiken

Hier ist das Abbild des Rasters «Restrisikomatrix» aus der Risikoanalyse einzufügen.



Die Nachfolgende Tabelle liefert eine Übersicht und Begründung zu den verbleibenden Risiken welche eine Einstufung von «rot» oder «gelb» aufweisen

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Risiko** | **Begründung** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Erhöhte Restrisiken (rot)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risiko-Nr. | Risiko | | | Bewertung |
|  |  | | |  |
| Massnahme(n) |  | | | |
| Umsetzungsgrad | % | Verantwortlich |  | |
| Umsetzung |  | | | |
| Ausstehend |  | | | |
| Bemerkung |  | | | |

### Erhöhte Restrisiken (gelb)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risiko-Nr. | Risiko | | | Bewertung |
|  |  | | |  |
| Massnahme(n) |  | | | |
| Umsetzungsgrad | % | Verantwortlich |  | |
| Umsetzung |  | | | |
| Ausstehend |  | | | |
| Bemerkung |  | | | |

## Besonders zu beachtende Punkte

Allfällige relevante Punkte aufführen

# Wiederherstellung des Geschäftsbetriebes

Bei einem Service, welcher kritische Geschäftsprozesse unterstützt, ist ein Notfallkonzept zu erstellen.

Dieses beschreibt die Notfallplanung und Katastrophenvorsorge Vertragsobjektes/Service, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.

# Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen

Beschreibt die Regelung zur Durchführung von angemeldeten oder unangemeldeten Revisionen und Überprüfungen der Informationssicherheitsaktivitäten im Projekt und anschliessend im Betrieb.

## Systemabnahmeprüfung

🡺 Neue und aktualisierte Systeme müssen während der Entwicklungsprozesse eine gründliche Überprüfung und Verifizierung erfahren, einschließlich der Vorbereitung einer detaillierten Planung der Aktivitäten, Testeingaben und erwarteten Ausgaben unter verschiedenen Bedingungen. Wie bei internen Entwicklungsvorhaben sollten derartige Prüfungen zunächst vom Entwicklungsteam durchgeführt werden. Danach sollten unabhängige Abnahmeprüfungen unternommen werden (sowohl bei internen als auch bei ausgelagerten Entwicklungsvorhaben), um sicherzustellen, dass das System wie erwartet (und nur wie erwartet) funktioniert (siehe ISO/IEC 27002:2013 Kapitel 14.1.1 und 14.1.2). Der Umfang der Prüfungen sollte der Bedeutung und der Beschaffenheit des Systems entsprechen.

Zusammenfassung des durchgeführten Audits (wer, wann, was, Resultat).

# Ausserbetriebnahme

Beschreibt die zu beachtenden Punkte bei der Ausserbetriebnahme wie Vernichtung von Datenträgern, Aufhebung von Berechtigungen, Anpassung von Zugriffsrechten etc.

# Abkürzungen

**Definitionen, Akronyme und Abkürzungen**

|  |  |
| --- | --- |
| Begriff / Abkürzung | Bedeutung |
| AV | Anwendungsverantwortlicher |
| DSBO | Datenschutzberater der Verwaltungseinheit |
| DSG | Eidgenössisches Datenschutzgesetz |
| EDÖB | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| ISBO | Informatiksicherheitsbeauftragter der Organisationeinheit |
| ISBD | Informatiksicherheitsbeauftragter des Departements |
| ISDS-Konzept | Informationssicherheits- und Datenschutzkonzept |
| NCSC | Nationales Zentrum für Cybersicherheit |
| Schuban | Schutzbedarfsanalyse |
| SLA | Service Level Agreement |
| SV | Systemverantwortlicher |
| VDSG | Verordnung zum Datenschutzgesetz |

# Anhang

Hier werden entsprechend weitergehende Dokumente angefügt, mindestens

* Schutzbedarfsanalyse
* Risikoanalyse