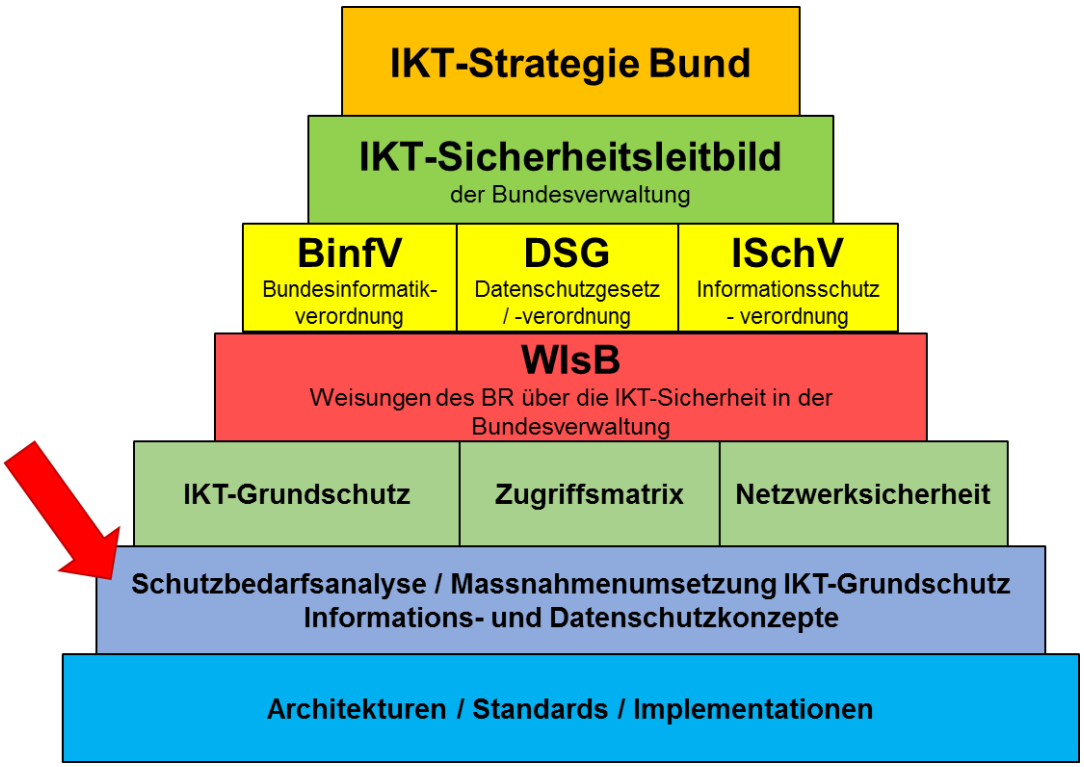
Version 4.3

P042 - Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

vom 19. Dezember 2013 (Stand 1. April 2019)

Das ISB erlässt gestützt auf Ziffer 3.1 der Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (WIsB) vom 16. Januar 2019 nachfolgende Vorgabe.



Inhalt

1 P042 - ISDS-Konzept

Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so ist zusätzlich zur Dokumentation der Umsetzung des IKT-Grundschutzes ein ISDS-Konzept mit Risikoanalyse zu erstellen[1]. Das ISB stellt jeweils die aktuelle Vorlage in Form eines Word-Dokuments zur Verfügung (*P042-Hi01- ISDS-Konzept*).

Die Erstellung der *ISDS-Konzepte* liegt in der Verantwortung des ISDS-Verantwortlichen (im Rahmen eines Projektes) oder des Anwendungsverantwortlichen.

Im ISDS-Konzept sind mindestens festzuhalten:

- Beschreibung des Schutzobjekts
- Verzeichnis der sicherheitsrelevanten Dokumente
- Einstufung nach WIsB
- Sicherheitsrelevante Systembeschreibung, inkl. Ansprechpartner / Verantwortlichkeiten, Beschreibung des Gesamtsystems, Beschreibung der zu bearbeitenden Daten (mit Verweis zum Bearbeitungsreglement gemäss Art. 21 VDSG wenn nötig), Architekturskizze / Kommunikationsmatrix, Beschreibung der zugrundeliegenden Technik
- Risikoanalyse und Schutzmassnahmen, inkl. Restrisiken die nicht oder ungenügend (reduziert) behandelt werden können – *dabei sind die vier Aspekte der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten zu berücktsichtigen*
- Wiederherstellung des Geschäftsbetriebes – *bei Schutzobjekten die kritische Geschäftsprozesse unterstützen*
- Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen, inkl. Systemabnahmeprüfung
- Liquidation
- Unterschriften von: ISBO, Auftraggeber, Geschäftsprozessverantwortlichen und Leiter der Verwaltungseinheit (oder einem Geschäftsleitungsmitglied) – *muss vor der Betriebsaufnahme erfolgen*

Weitere Angaben können individuell gefordert bzw. hinzugefügt werden.

1.1 Gültigkeit des ISDS-Konzeptes

Die Gültigkeit des ISDS-Konzepts beträgt maximal 5 Jahre.

[1] WIsB Art 3.2 Abs. 4

2 Hilfsmittel zur Umsetzung von P042

Bei der Erfassung des ISDS-Konzepts sind verschiedene Dokumente zu berücksichtigen und zu erstellen:

- Das ISDS-Konzept per se;
- die Risikoanalyse;
- das Notfallkonzept;
- das Bearbeitungsreglement.

Die Hauptbearbeitung dieser Dokumente findet vorzugweise während der Konzeptphase statt.

Für jedes Dokument steht ein Hilfsmittel zur Verfügung: Dieses entspricht einem Dokumenten-Template mit dessen Hilfe die Vorgaben richtig umgesetzt werden können. Alle genannten Dokumente sind bei Änderungen (am Schutzobjekt) zu prüfen und wenn nötig anzupassen. Nach maximal 5 Jahren müssen sie zwingend neu bearbeitet werden.[2]

Diese Dokumentation muss durch den ISBO, den Auftraggeber, den Geschäftsprozessverantwortlichen und den Leiter der Verwaltungseinheit (oder einem Geschäftsleitungsmitglied) vor der Betriebsaufnahme unterschrieben werden.

2.1 P042-Hi01 - ISDS-Konzept

Das *ISDS-Konzept* gilt als Hauptdokument der Informationssicherheit und des Datenschutzes im Projekt und während des Betriebes. Es legt die nötigen Angaben zur Erhaltung und Verbesserung der Informationssicherheit und des Datenschutzes fest und fasst die Aspekte der Informationssicherheit und des Datenschutzes im Projekt zusammen.
Das *ISDS-Konzept* enthält u. a. eine Zusammenfassung und Beurteilung der bekannte Restrisiken, die durch die verantwortlichen Stellen in Kauf genommen werden müssen.[3] Es enthält auch eine Beschreibung der sicherheitsrelevanten Funktionalitäten des Gesamtsystems. Die Ausserbetriebnahme ist auch zu berücksichtigen.

Das ISDS-Konzept kann bei sicherheitsrelevanten Systemen nicht weggelassen werden. Gewisse Unterkapitel können jedoch wegfallen, falls diese nicht relevant sind.

2.2 P042-Hi02 - Risikoanalyse

Die *Risikoanalyse* ist eine Beschreibung der relevanten Risikofaktoren (Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit) und eine Auflistung und Bewertung der Risiken. Sie zeigt ein Bild über das vorhandene Risikopotential des untersuchten Systems auf.

2.3 P042-Hi03 - Notfallkonzept

Gemäss Massnahme 17.1.1 des IKT-Grundschutzes müssen Pläne für die Sicherstellung des Geschäftsbetriebes entwickelt, dokumentiert und umgesetzt werden. Das *Notfallkonzept* beschreibt die Notfallplanung und Katastrophenvorsorge, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.
Dazu stellt das ISB den Verwaltungseinheiten und Projektleitern ein Hilfsmittel (Template) für ein Notfallkonzept zur Verfügung.

[2] IKT-Grundschutz Massnahme. 1.1.2
[3] WIsB Art 3.4 Abs. 1

2.4 P042-Hi04 - Bearbeitungsreglement

Das Bearbeitungsreglement sorgt für die notwendige Transparenz im Umfeld der Systementwicklung und der Datenbearbeitung.
Die Grundlage des *Bearbeitungsreglements* - im Rahmen von IKT-Vorhaben der Bundesverwaltung - ist das ISDS-Konzept. Der Inhaber einer automatisierten Datensammlung erstellt ein Bearbeitungsreglement, wenn diese Datensammlung (siehe Art. 21 VDSG):

- besonders schützenswerte Personendaten oder Persönlichkeitsprofile beinhaltet;
- durch mehrere Bundesorgane benutzt wird;
- Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht wird; oder
- mit anderen Datensammlungen verknüpft ist.

Das Bearbeitungsreglement soll für die notwendige Transparenz im Rahmen der Systementwicklung, -adaption wie auch der **elektronischen Bearbeitung von Personendaten** sorgen.