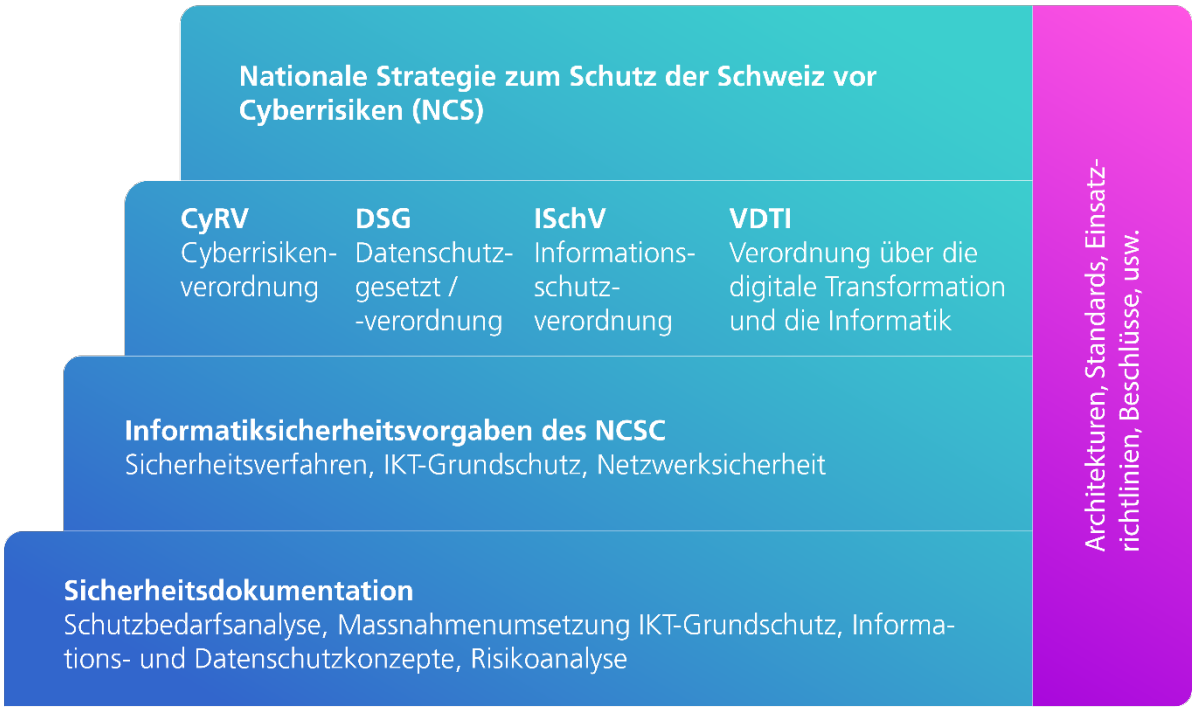
Version 4.4

P042 - Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

vom 19. Dezember 2013 (Stand 1. April 2021)

Der Delegierte für Cybersicherheit erlässt gestützt auf Artikel 11, Absatz 1, Buchstabe e der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) vom 27. Mai 2020 nachfolgende Vorgabe. Diese stellt eine Vorgabe für den erhöhten Schutz gemäss Artikel 14d CyRV dar.



Inhalt

1 P042 - ISDS-Konzept

Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so definieren die Verwaltungseinheiten, zusätzlich zur Umsetzung der Sicherheitsvorgaben für den Grundschutz und basierend auf einer Risikoanalyse, weitere Sicherheitsmassahmen, dokumentieren diese und setzten sie um (Art.14d Abs.1 CyRV). Das ISDS-Konzept beinhaltet die Beschreibung der Sicherheitsmassnahmen und ihrer Umsetzung für das Informatikschutzobjekt sowie der Restrisiken.

Die Erstellung des ISDS-Konzepts liegt in der Verantwortung des ISDS-Verantwortlichen (im Rahmen eines Projektes) oder des Anwendungsverantwortlichen. Bei der Erstellung des ISDS-Konzepts darf auf bestehende themenspezifische Sicherheitskonzepte verwiesen werden. Das NCSC stellt jeweils eine aktuelle Vorlage in Form eines Word-Dokuments zur Verfügung (*P042-Hi01- ISDS-Konzept*).

Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichteten Verwaltungseinheiten (VE) zu dokumentieren und zu überprüfen (CyRV, Art.14 Abs. 3 und Art.14d).
Die Sicherheitsanforderungen sind mit den Leistungserbringern sowohl für die Entwicklung und den Betrieb als auch für die Ausserbetriebnahme von Informatikmitteln schriftlich zu vereinbaren. Die Verwaltungseinheiten dokumentieren und überprüfen die Umsetzung der Sicherheitsmassnahmen.

Das ISDS-Konzept ist mindestens von der oder dem Informatiksicherheitsbeauftragten der Verwaltungseinheit (ISBO) zu prüfen[1]. Sie ist von der Auftraggeberin oder dem Auftraggeber und dem oder der Geschäftsprozessverantwortlichen zu genehmigen.

Die Verwaltungseinheiten weisen Risiken aus, die nicht oder nur ungenügend reduziert werden können (Restrisiken), und dokumentieren diese. Die Projektauftraggeberin oder der Projektauftraggeber, die oder der Geschäftsprozessverantwortliche sowie die Leitung der Verwaltungseinheit nehmen die Restrisiken zur Kenntnis und bestätigen dies schriftlich. (Art.14d Abs.2 CyRV)
Der Entscheid darüber, ob bekannte Restrisiken in Kauf genommen werden, obliegt der Leiterin oder dem Leiter der zuständigen Verwaltungseinheit. (Art.14d Abs.3 CyRV)

Im ISDS-Konzept sind mindestens festzuhalten:

- Beschreibung des Informatikschutzobjekts
- Verzeichnis der sicherheitsrelevanten Dokumente
- Einstufung nach P041 - Schutzbedarfsanalyse
- 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 Sicherheitsmassnahmen, inkl. Risiken die nicht oder nur ungenügend reduziert werden können (Restrisiken) – *dabei sind die vier Aspekte der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten zu berücktsichtigen*
- Wiederherstellung des Geschäftsbetriebes – *bei Informatikschutzobjekten die kritische Geschäftsprozesse unterstützen*

[1] Bei den Standarddiensten ist es von der oder dem Informatiksicherheitsbeauftragten für die Standarddienste zu prüfen.

- Einhaltung / Überprüfung / Abnahme der Sicherheitsmassnahmen, 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.

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 (bei Informatikschutzobjekten, die kritische Geschäftsprozesse unterstützen*)*;
- das Bearbeitungsreglement (wenn nötig gemäss Art. 21 VDSG).

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. Ihre Nutzung (insbesondere der Inhalt) kann für die eigenen Bedürfnisse und Ziele angepasst werden. Die Vorlagen sind so zu verstehen, dass sie ein Hilfsmittel sind, um alle Sicherheitsvorgaben richtig einzuhalten. Sie dienen als Checkliste für die Berücksichtigung aller sicherheitsrelevanten Aspekte. Alle genannten Dokumente sind bei Änderungen (am Informatikschutzobjekt) 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* be-

[2] Art.14e CyRV
[3] Art.14d CyRV

schreibt die Notfallplanung und Katastrophenvorsorge, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.
Dazu stellt das NCSC den Verwaltungseinheiten und Projektleitern ein Hilfsmittel (*Template*) für ein Notfallkonzept zur Verfügung.

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 IT-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.