|  |  |
| --- | --- |
|  | Wenn ausgefüllt mindestens: INTERN |

|  |
| --- |
|  |

P042-Hi01 - Informationssicherheits- und

Datenschutzkonzept (ISDS-Konzept)

<Projektname / Schutzobjektname>

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Klassifizierung | INTERN / VERTRAULICH / GEHEIM |
| Status | in Arbeit / in Prüfung / genehmigt zur Nutzung |
| Projektnummer |  |
| Projektleiter (PL LB) |  |
| Version | Aus Template V4.4 |
| Datum |  |
| Auftraggeber |  |
| Autor/Autoren |  |

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Verteiler

|  |  |  |
| --- | --- | --- |
| Funktion | Name | Departement / Amt |
| ISBO |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Prüfung des Dokuments nach den Projektphasen

Die Tabellen mit Personen die die einzelnen Phasen einsehen (bestätigen) können beliebig ergänzt werden.

Initialisierung – vor Projektfreigabe

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Funktion | Name | Datum |
|  | ISDS-V |  |  |
| ISBO |  |  |
|  |  |  |

Konzept – vor Phasenfreigabe

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Funktion | Name | Datum |
|  | ISDS-V |  |  |
| ISBO |  |  |
|  |  |  |

Realisierung – vor Phasenfreigabe

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Funktion | Name | Datum |
|  | ISDS-V |  |  |
| ISBO |  |  |
|  |  |  |

Einführung – vor Betriebsaufnahme

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Funktion | Name | Datum |
|  | ISDS-V |  |  |
| ISBO |  |  |
|  |  |  |

Inhaltsverzeichnis

1 Generelle Anmerkungen 5

1.1 Beschreibung 5

1.2 Zweck des Dokuments 5

1.3 Gültigkeit des Dokuments 5

2 Management Summary 6

2.1 Allgemeines 6

2.2 Zusammenfassung Restrisiken 6

2.3 Abschliessende Bemerkungen 6

2.4 Genehmigung 7

3 Verzeichnis der sicherheitsrelevanten Dokumente 8

4 Einstufung nach P041 - Schutzbedarfsanalyse 8

5 Sicherheitsrelevante Systembeschreibung 10

5.1 Ansprechpartner / Verantwortlichkeiten 10

5.2 Beschreibung des Gesamtsystems 10

5.3 Beschreibung der zu bearbeitenden Daten 10

5.4 Architekturskizze / Kommunikationsmatrix 11

5.5 Beschreibung der zugrundeliegenden Technik 12

6 Risikoanalyse und Schutzmassnahmen 13

6.1 Restrisiken 13

7 Wiederherstellung des Geschäftsbetriebes 14

8 Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen 14

8.1 Systemabnahmeprüfung 14

9 Ausserbetriebnahme 14

10 Abkürzungen 15

11 Anhang 15

# Generelle Anmerkungen

**Hinweise zum Ausfüllen des Dokuments**

Der Sicherheitsprozess hat die konkrete Berücksichtigung der Informatiksicherheit in Projekten, bei der Einführung und der Nutzung von Informatikmitteln, zum Ziel. Um dieses sicherzustellen, werden spezifische Dokumentationen verlangt. Dafür stellt das NCSC entsprechende Vorlagen zur Verfügung. Ihre Nutzung (insbesondere der Inhalt) kann auf 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.

* Schwarze Texte sind Textbausteine, die die Vorgaben entsprechen. Diese sollten, so weit sie Sinn machen, übernommen und nicht geändert werden.
* Blaue Texte dienen als Hilfe zum Ausfüllen des Dokumentes. Der Text soll nach dem Einfüllen eines entsprechenden konkreten projektbezogenen Textes gelöscht werden.
* Rote Texte sind wichtige Hinweise oder Fragestellungen die speziell abzuklären sind oder konkret beschrieben werden müssen.
* Wenn die Einstufung gemäss Kapitel 4 (Einstufung nach P041 - Schutzbedarfsanalyse) keinen erhöhten Schutzbedarf ergibt und man trotzdem ein ISDS-Konzept schreiben muss (z.B. als Konsequenz oder Ausnahme zum IKT-Grundschutz), kann die Risikoanalyse (gemäss Kapitel 6) weggelassen werden.

## Beschreibung

Beschreibung des Schutzobjekts

## 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 im Projekt zusammen.

Für eine korrekte Grundlage eines IKT-Vorhabens sind die Artikel 4, Absatz 1 und Artikel 14, Absatz 3 der CyRV ein wesentlicher Bestandteil.

Sämtliche Sicherheitsmassnahmen für die einzelnen Informatikschutzobjekte müssen in aktueller Form dokumentiert werden (nach Art. 14, Abs. 3 CyRV). Dazu dient unter anderem dieses ISDS-Konzept (Art.14d, Abs.1 CyRV).

## Gültigkeit des Dokuments

Die Gültigkeit eines ISDS-Konzepts beträgt maximal 5 Jahre.

# Management Summary

Das Management Summary sollte so formuliert sein, dass es auch für Personen verständlich ist, welche nicht über vertiefte technische Kenntnisse verfügen («in der Sprache des Geschäfts»).

## 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 dem Leiter der zuständigen Verwaltungseinheit.

## Abschliessende Bemerkungen

Abschliessende wichtige Bemerkungen und Fazits zum vorliegenden Informatikschutzobjekt.

## Genehmigung

Die Unterschriften zur Genehmigung und zur Akzeptanz der verbleibenden Risiken müssen vor der Betriebsaufnahme geleistet werden.

Mit seiner Unterschrift bestätigt der Informatiksicherheitsbeauftrage (ISBO) das ISDS-Konzept geprüft zu haben. Sie oder er hat insbesondere geprüft ob das Dokument vollständig ausgefüllt ist und alle geforderten Massnahmen dokumentiert sind. Sie oder er hat die Angaben kritisch hinterfragt, ob sie konsistent sind und im Kontext des Informatikschutzobjektes stimmen.

Der Auftraggeber und der Geschäftsprozessverantwortlicher genehmigen mit ihrer Unterschrift das ISDS-Konzept.

Der Leiter der zuständigen Verwaltungseinheit entscheidet, ob bekannte Restrisiken in Kauf genommen werden können[[1]](#footnote-1). Das Dokument kann, je nach amtsinterner Regelung, auch von einem anderen verantwortlichen Mitglied der Geschäftsleitung unterzeichnet werden.

|  |  |
| --- | --- |
| Datum / Name / Unterschrift  **ISBO**: | …………………………………………………...…... |
| Datum / Name / Unterschrift  **Auftraggeber**: | …………………………………………………...…... |
| Datum / Name / Unterschrift  **Geschäftsprozessverantwortlicher**: | …………………………………………………...…... |
| Datum / Name / Unterschrift  **Leiter/in VE oder GL-Mitglied**: | …………………………………………………...…... |

**Weitere Unterschriften, zum Beispiel die des Verantwortlichen beim LE, können hinzugefügt werden.**

**Die Unterschriften können auch in elektronischer Form (in einem PDF) angebracht werden.**

# **Verzeichnis der sicherheitsrelevanten Dokumente**

Hier sind die rechtlichen Grundlagen anzuführen auf die sich das (zu realisierende) IT-Vorhaben abstützt. Die Erhebung dieser Grundlagen geschieht von Vorteil im Zusammenarbeit mit dem Rechtsdienst der Verwaltungseinheit oder des Departements.

Unter dem Link <http://www.hermes.admin.ch/onlinepublikation/index.xhtml?element=ergebnis_rechtsgrundlagenanalyse.html> ist ein Muster zur Dokumentation der entsprechenden Rechtsgrundlagen.

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

Sie ist durch die departements- und/oder amtseigenen Dokumente zu ergänzen.

|  |  |
| --- | --- |
| 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 | SR 120.73 [Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV)](https://www.admin.ch/opc/de/classified-compilation/20200291/index.html) |
|  | [SR 510.411 Informationsschutzverordnung (ISchV)](http://www.admin.ch/ch/d/sr/c510_411.html) |
|  | [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 |  |
|  |  |
| Strategie | [IKT-Strategie der Bundesverwaltung](https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb000-ikt-strategie-des-bundes.html) |
|  |  |
| Methode | [HERMES - Die schweizerische Projektführungsmethode](http://www.hermes.admin.ch/) |
|  |  |
| Übergeordnete Sicherheitskonzepte |  |
| SLA |  |
|  |  |
| weitere | 🡺 Vom Verfasser zu ergänzen |

# Einstufung nach P041 - Schutzbedarfsanalyse

Die Einstufung des Informatikschutzobjekts muss gemäss Schutzbedarfsanalyse (Schuban),   
[P041 - Schutzbedarfsanalyse (Schuban)](https://intranet.ncsc.admin.ch/ncscintra/de/home/vorgaben-hilfsmittel/sicherheitsverfahren/beurteilung-schutzbedarf.html), vorgenommen werden.

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

Das Ergebnis der genehmigten Schutzbedarfsanalyse ist hier in geeigneter Form abzubilden (die komplette Schutzbedarfsanalyse kann z.B. im Anhang aufgeführt werden).

# Sicherheitsrelevante Systembeschreibung

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

## Ansprechpartner / Verantwortlichkeiten

|  |  |
| --- | --- |
| Wer | Name |
| Anwendungsverantwortlicher |  |
| Inhaber der Daten |  |
| Systembetreiber LE |  |
| Projektleiter LB |  |
| Ansprechpartner beim LE |  |
| ISBD |  |
| ISBO |  |
| DSBO |  |
| Benutzerkreis |  |
| weitere Stellen |  |

## Beschreibung des Gesamtsystems

Beschreibung 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:

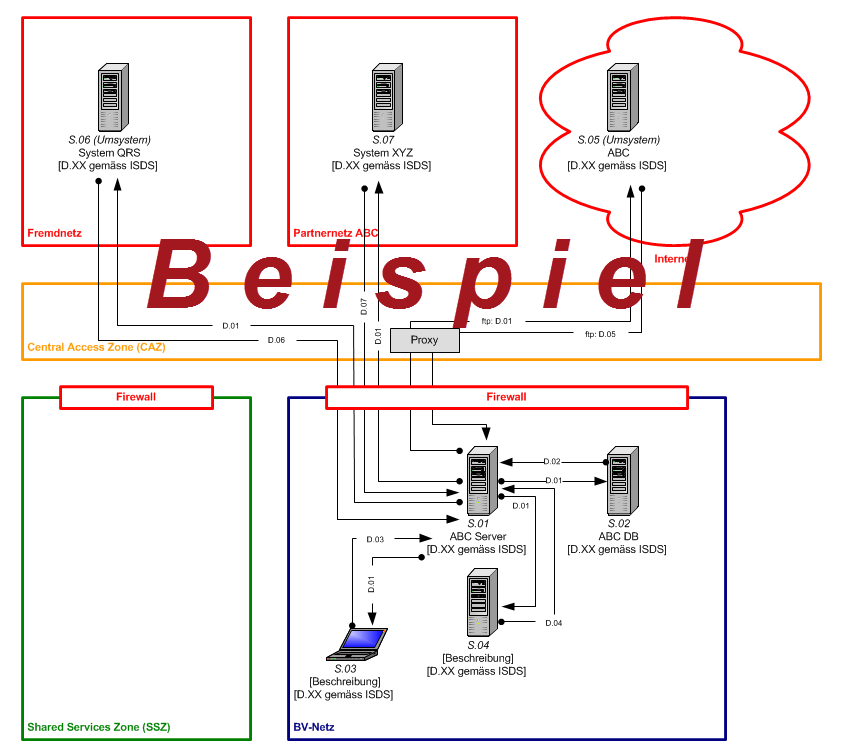
* Ist die Datensammlung beim EDÖB angemeldet?

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
* Wenn das Schutzobjekt RINA-relevant ist, dann ist hier ein Verweis zur entsprechenden Dokumentation anzubringen.

## Architekturskizze / Kommunikationsmatrix

Hier ist eine Architekturskizze und eine Kommunikationsmatrix einzufügen. Oder es ist hier auf das entsprechende aktuell gehaltene Dokument zu 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.

Oder es ist hier auf das entsprechende aktuell gehaltene Dokument zu verweisen.

# Risikoanalyse und Schutzmassnahmen

Beschreibung der relevanten Risikofaktoren (Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit), Auflistung und Bewertung der Risiken, inkl. der Risiken aus einer möglichen RINA-Relevanz.

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

Ergebnisse aus der Risikoanalyse:

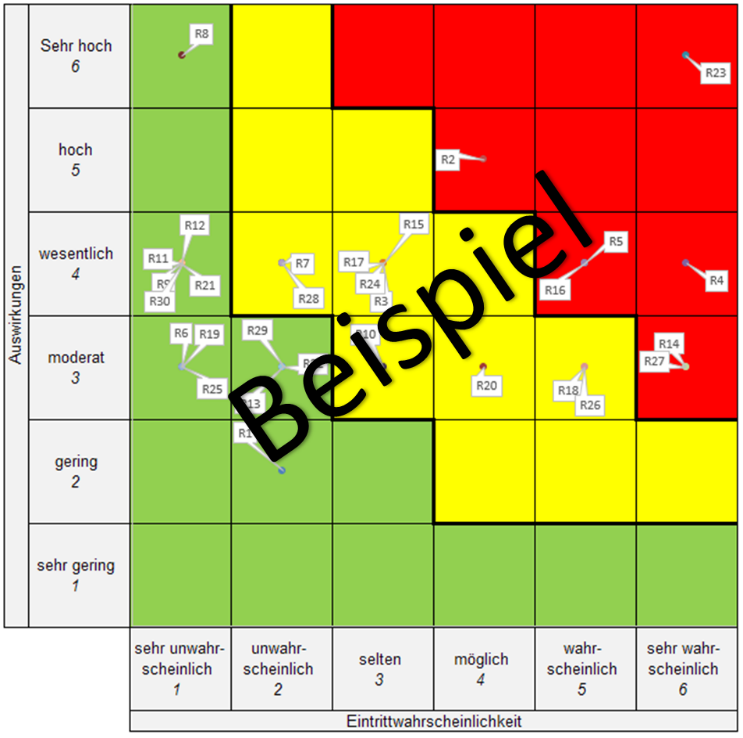
In der Arbeitsmappe «Restrisikomatrix» ist beschrieben, in welcher Kategorie sich das beurteilte Restrisiko befindet.

* Grün: sind Risiken die entweder inhärent (im Schutzobjekt als solches) 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 Managementsummary (Kapitel 2.2) kurz zusammengefasst werden.

## Restrisiken

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



In der folgenden Tabelle ist eine Begründung zu den verbleibenden Risiken (rot und gelb markierte Risiken) einzufügen.

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

# Wiederherstellung des Geschäftsbetriebes

Bei einem Schutzobjekt, das kritische Geschäftsprozesse unterstützt, ist ein Notfallkonzept zu erstellen.

Dies beschreibt die Notfallplanung und Katastrophenvorsorge des Informatikschutzobjekts, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten. Eine Hilfestellung dazu ist im Dokument «P042-Hi03 - Notfallkonzept»[[2]](#footnote-2) zu finden..

In jedem Fall ist hier ein Verweis zu den BCM Dokumenten auf Stufe Amt zu machen.

# 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.

# 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 |
| ISDS-V | Informationssicherheits- und Datenschutzverantwortlicher im Rahmen des Projekts, gemäss HERMES |
| NCSC | Nationales Zentrum für Cybersicherheit |
| PL | Projektleiter |
| RINA | Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung |
| Schuban | Schutzbedarfsanalyse |
| SLA | Service Level Agreement |
| SV | Systemverantwortlicher |
| VDSG | Verordnung zum Datenschutzgesetz |

# Anhang

Hier werden entsprechend weitergehende Dokumente angefügt, mindestens

* P041-Hi01-Schutzbedarfsanalyse
* P042-Hi02- Risikoanalyse

1. Art.14d, Abs.3 CyRV [↑](#footnote-ref-1)
2. [intranet.ncsc.admin.ch](intranet.ncsc.admin.ch/), Vorgaben & Hilfsmittel > Sicherheitsverfahren > Erhöhter Schutz > P042 - Informationssicherheits- und Datenschutzkonzept (ISDS) [↑](#footnote-ref-2)