**Projekt: ……………………………..**

**Informationssicherheits- und
Daten­schutzkonzept (ISDS-Konzept)**

***Vorlage***

Version 1.2, Mai 2021

Änderungsverzeichnis

| Datum  | Version | Änderung | Autor |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Inhalt

[1. Zusammenfassung 3](#_Toc72504574)

[2. Einleitung 3](#_Toc72504575)

[2.1. Ziel des ISDS 3](#_Toc72504576)

[2.2. Geltungsbereich / Abgrenzung 3](#_Toc72504577)

[2.3. IT-Grundschutz 3](#_Toc72504578)

[2.4. Ansprechpartner und Verantwortlichkeiten 4](#_Toc72504579)

[3. Rechtsgrundlagen 4](#_Toc72504580)

[4. Einstufung aufgrund der Schutzbedarfsanalyse 4](#_Toc72504581)

[5. Sicherheitsrelevante Systembeschreibung 5](#_Toc72504582)

[5.1. Gesamtsystem / Applikation 5](#_Toc72504583)

[5.2. Datenbearbeitung 6](#_Toc72504584)

[6. Risikoanalyse 6](#_Toc72504585)

[7. Schutzmassnahmen 9](#_Toc72504586)

[7.1. Authentisierung 9](#_Toc72504587)

[7.2. Autorisierung (Benutzer- und Zugriffsrechte 10](#_Toc72504588)

[7.3. Logging und Monitoring 10](#_Toc72504589)

[8. Sicherstellung des Geschäftsbetriebs inkl. Notfallkonzept 10](#_Toc72504590)

[8.1. Wartung / Change Management 10](#_Toc72504591)

[8.2. Notfall Konzept (Business Continuity Mgmt BCM) 11](#_Toc72504592)

[9. Einhaltung / Überprüfung der Schutzmassnahmen 11](#_Toc72504593)

[10. Abnahme 11](#_Toc72504594)

[11. Anhang: Risikomatrix 12](#_Toc72504595)

[11.1. Risikomatrix Kanton 12](#_Toc72504596)

[11.2. Risikomatrix Nicht-Kanton 14](#_Toc72504597)

# Zusammenfassung

* *Dieses Template dient als Hilfestellung für die Erstellung eines ISDS-Konzeptes. Es besteht nicht der Anspruch, dass im Einzelfall alle in diesem Template genannten Themen abgehandelt werden müssen. Ebenso kann das Template nicht als vollständige Auflistung aller abzuhandelnden Bereiche angesehen werden.*

# Einleitung

## Ziel des ISDS

* Das Informationssicherheits- und Datenschutzkonzept- (ISDS) beschreibt die sicherheitsrelevanten Aspekte des Projektes und des späteren Betriebs der IT-Infrastruktur. Die Schwerpunkte der Betrachtung liegen auf:
	+ den Rechtsgrundlagen
	+ dem Schutzbedarf und den Sicherheitsvorgaben
	+ der sicherheitsrelevanten Projektbeschreibung;
	+ der Analyse der Risiken;
	+ und dem Handlungsbedarf (zu ergreifenden Massnahmen).

## Geltungsbereich / Abgrenzung

Hier können allfällige existierende Systeme oder Schnittstelle vom ISDS-Konzept abgegrenzt werden und/oder Verweise auf andere ISDS-Konzepte etc. eingefügt werden.

## IT-Grundschutz

* *Wie wird der IT-Grundschutz sichergestellt?*
* *Wo sind die konkreten Massnahmen definiert (Verweis)?*
* *Allfällige Zertifizierungen aufführen*

Die Anforderungen für die Beurteilung und Behandlung der grundlegenden Informationssicherheitsrisiken im Falle von On-Premises-Lösungen (IT-Grundschutz) sind generell zu regeln (z.B. bei der kantonalen Verwaltung im Managementsystem des AIO unter Anwendung der ISO Norm 27001). Hierzu gehören insbesondere: Rechenzentrum, Netzwerksicherheit, Sicherheitsaspekte der (persönlichen) PCs, Laptops, Smartphones und Tablets der Mitarbeiter (z.B. Passwort-Regeln, Virenschutz, Verschlüsselung der Harddisks) etc.

Wird die Anwendung in der kantonalen IT-Infrastruktur betrieben, muss der Grundschutz *nicht* beschrieben werden.

## Ansprechpartner und Verantwortlichkeiten

|  |  |  |  |
| --- | --- | --- | --- |
| **Rolle**  | **Kontakt**  | **Abteilung, Firma**  | **Aufgaben**  |
| Dateninhaber |  |  |  |
| Anwendungsverantwortlicher |  |  |  |
| Systembetreiber  |  |  |  |
| IT Sicherheitsbeauftragter  |  |  |  |

# Rechtsgrundlagen

*Siehe separates Dokument Rechtsgrundlagenanalyse*

* *Nennung der konkret relevanten Rechtsgrundlagen*

# Einstufung aufgrund der Schutzbedarfsanalyse

* *Verweis auf das separat erstellte Dokument* [*Schutzbedarfsanalyse*](https://izug.zg.ch/web/behoerden/datenschutzstelle/services/datenschutz-folgenabschaetzung/dokumente-zur-dsfa/schutzbedarfsanalyse/download)
* *Zusammenfassende Darstellung des Schutzbedarfs, u.a. bezüglich Datenschutz und Datensicherheit*
* *Aufführen der sich aus dem Schutzbedarf ergebenden groben Anforderungen (Vorgehen und inhaltlich)*

# Sicherheitsrelevante Systembeschreibung

* Gesamtübersicht der Systembeschreibung inkl. Funktionen und Datenflüsse (z.B. Use Cases) *Für weiterführende Details kann auf separate Dokumentationen verwiesen werden.*
* *Wichtig: Ein ISDS-Konzept muss die individuell geplante Lösung und entsprechend die konkreten Konfigurationen / Parametrierungen abbilden. Ein ISDS-Konzept seitens Hersteller, welches allgemein gehalten oder Umsetzungsoptionen offenlässt, genügt nicht.*

## Gesamtsystem / Applikation

* *Beschreibung des Gesamtsystems, idealerweise in Form einer Architekturskizze
Beispiel:*
* *Welche Technologien werden eingesetzt?*
* *An welchen Standorten (inhouse/extern, Länder) befinden sich die eingesetzten Komponenten?*
* *Aufzeigen genutzter Netzwerke*
* *Allfällige Schnittstellen zu Drittsystemen / Drittstellen aufzeigen*
* *Wer betreibt welche Komponenten, gibt es Subakkordanten, in welchen Ländern sind diese Firmen angesiedelt?*
* *Im Falle von mehreren Nutzern: Wie ist die Mandantenfähigkeit sichergestellt?*
* *etc.*

## Datenbearbeitung

* *Datenflussdiagramm (sofern nicht bereits in Datenschutz-Folgenabschätzung enthalten) – welche Daten werden wo und wann bearbeitet/gespeichert/übermittelt?*
* *Aufzeigen des Datenlebenszyklus, d.h. von der Entstehung bis zur Löschung*
* *Wie und wo werden Daten übermittelt? Wie werden sie verschlüsselt?*
* *etc.*

# Risikoanalyse

* *Grundlage bildet die Risikoanalyse der separaten* Datenschutz-Folgenabschätzung *(Datenschutz-Folgenabschätzung ist «high level», in diesem ISDS-Konzept sind konkretere technische, organisatorische und allenfalls vertragsrechtliche Risiken aufzuführen).*
* *Aufzuführen sind Risiken auf der Detailstufe bezogen auf die gewählte Architektur zu den Themen Verfügbarkeit, Integrität und Vertraulichkeit insbesondere zu
- Zugriffs-/Anmeldeverfahren
- Nachvollziehbarkeit wesentlicher Aktivitäten, z.B. Login, Datenzugriff, -veränderung, -löschung, etc.
- Schnittstellen zu Umsystemen
- etc*

***Methodik*** *(siehe Kap. 11)*

1. **Inhärentes Risiko**: Welche Risiken sind mit der geplanten oder geänderten Bearbeitung von Personendaten verbunden?
*Die Risiken sind ohne die Berücksichtigung von möglichen geplanten Massnahmen aufzuführen (inhärentes Risiko).*
2. **Risikobewertung:** Wie sind die identifizierten Risiken in Bezug auf das Schadensausmass und die Eintretenswahrscheinlichkeit zu bewerten? Die Risikobewertung erfolgt nach der in Kap. 11 beschriebenen Methodik.
*Bei der Risikobewertung wird ebenfalls die Annahme getroffen, dass keine risikomindernden Massnahmen getroffen worden sind.*
3. **Massnahmen:** Welche Massnahmen zur Bewältigung des identifizierten Risikos werden getroffen?
4. **Bewertung Restrisiko:** Welches Risiko bleibt nach Berücksichtigung der vorgesehenen Massnahme (Spalte C) bestehen?

| *#* | *A)* *Inhärentes Risiko* | *B) Bewertung* | *C) Massnahme (Beschreibung unter Kap. 7)* | *D) Restrisiko* |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Schutzmassnahmen

* *Verweise auf allfällig separat erstelle Dokumente*
* *Wichtig: Ein ISDS-Konzept muss die individuell geplante Lösung und entsprechend die konkreten Konfigurationen / Parametrierungen abbilden. Ein ISDS-Konzept seitens Hersteller, welches allgemein gehalten oder Umsetzungsoptionen offenlässt, genügt nicht.*
* *Schutzmassnahmen sind immer auf den drei Schichten a) Geschäftsprozesse, b) Fachanwendungen und c) IT-Systeme umzusetzen.

 *

## Authentisierung

* *Anwenderkreis*

|  |  |  |  |
| --- | --- | --- | --- |
| **Anwenderkreise** | **Clienttyp / Rechte** | **Authentisierungsangaben** | **Bemerkung / Aufgaben** |
| Administratoren / externe Supportfirmen |  |  |  |
| Mitarbeitende IT-Betrieb (Helpdesk) |  |  |  |
| Mitarbeitende (internes Netzwerk)  |  |  |  |
| Öffentlichkeit mit Login |  |  |  |
| Etc. |  |  |  |

* *Beschreibung der Authentisierungsverfahren (Wo meldet sich der User an)*
* *Wie erfolgt die Anmeldung (Arbeitsplatz-Login separates Login oder SingleSignOn)?*
* *Prozessbeschreibung der verschiedenen Anwendungsfälle rund um die Authentisierung (Vergabe Initialpasswort, Rücksetzung, etc.)*

## Autorisierung (Benutzer- und Zugriffsrechte

* *Wer hat mit welchen Rechten auf welchen Daten Zugriff?*
* *Wie sehen die Betriebsprozesse für Kontoeröffnung, Rechtevergabe bzw. -löschung aus?*
* *Gibt es ein (rollenbasiertes) Berechtigungskonzept?*
* *etc.*

## Logging und Monitoring

* *Beschreibung wo und wie lange Aktivitäten aufgezeichnet werden, Zweck und Zugriffsrechte auf die Log-Daten.*
* *Bei Monitoring: Beschreibung der Mechanismen,*

## Weitere Schutzmassnahmen

* *Beschreibung der technischen, organisatorischen und vertraglichen Massnahmen gemäss Kap. 6 Risikoanalyse und allfälliger weiterer Massnahmen.*

# Sicherstellung des Geschäftsbetriebs inkl. Notfallkonzept

## Wartung / Change Management

* *Beschreibung der erforderlichen System Wartung / Change Managementprozess wie Release Update.*

## Notfall Konzept (Business Continuity Mgmt BCM)

* *Beschreibung der Massnahmen wie Wiederanlauf / Restore*

# Einhaltung / Überprüfung der Schutzmassnahmen

* *Wie wird sichergestellt, dass die definierten Massnahmen umgesetzt, aktuell gehalten und laufend wirksam sind?*

# Abnahme

* *Abnahme durch den zuständigen IT-SIBE*

# Anhang: Risikomatrix

## Risikomatrix Kanton

Die in diesem Kapitel beschriebene Risikomatrix ist von der Finanzdirektion vorgegeben und gilt für alle kantonalen Amtsstellen. Anderen Organen steht es frei, alternativ mit der vereinfachten in Kap. 11.2 beschriebenen Risikomatrix zu arbeiten.

Folgend die wichtigsten Angaben zur Risikobewertung in der Übersicht:



Eintrittswahrscheinlichkeit (E):

|  |
| --- |
|  |

Schadensausmass (S):

|  |
| --- |
|  |

Das Schadensausmass wird nicht nur monetär beurteilt, sondern eingerechnet sind auch Reputationsschaden und allfällige Gerichtskosten.

*Übertragen in die Risikoanalyse des ISDS-Konzeptes wird «nur» der Wert Schadensausmass \* Eintretenswahrscheinlichkeit gemäss Matrix .* Beispiele: E=3 \* S=2 = 6 (Gelb) oder E=1 \* S=6 = 6 (Orange)*.*

## Risikomatrix Nicht-Kanton

Organe ausserhalb der kantonalen Verwaltung können anstelle der im vorangehenden Kapitel beschriebenen Risikomatrix die hier dargestellt vereinfachte Version verwenden. Für die Unterscheidung von tief/mittel/hoch wird dabei keine vorgegebene Skala verwendet.

