ISDS-Fragebogen für Dienstleister V0.2

07.11.2025 Der ISDS-Fragebogen ist in der Version 0.2 vorhanden und wird fortlaufend weiterentwickelt.

Informationen zum Ausfüllen

Fragekategorien:

- Erforderlich gekennzeichnete Fragen
  - Müssen zwingend beantwortet werden.
  - Falls nicht anwendbar, ist dies explizit zu kennzeichnen und nachvollziehbar zu begründen.
  - Bewertung:
    - Angemessen beantwortet → risikomindernd
    - Unangemessen beantwortet → als Restrisiko ausgewiesen
    - Nicht beantwortet → als Risiko ausgewiesen
- Optionale gekennzeichnete Fragen
  - Eine Beantwortung ist freiwillig.
  - Trägt positiv zur Bewertung der informationssicherheitsrelevanten Gesamtsituation bei.

Fokus der Fragen (siehe Überschrift)

- Applikationsfokus
  - Bezieht sich ausschliesslich auf die betrachtete Applikation.
  - Entsprechend soll die Frage aus der Perspektive der Applikation beantwortet werden.
- Dienstleisterfokus
  - Bezieht sich auf die gesamte Organisation des Dienstleisters.
  - Entsprechend soll die Frage aus der Perspektive des Unternehmens beantwortet werden.

Form der Antworten

- Fragen mit textlicher Beschreibung erfordern eine ausführliche und inhaltlich präzise Beantwortung.

Bewertungssystem und Transparenz

- Alle Risiken zu den Fragen sind vorab definiert und unter folgendem Link einsehbar: https://explore.educa.ch/risikodatenbank/

Inhaltsverzeichnis

Allgemein

Applikations- und Dienstleisterbeschrieb

Erforderlich: Welches ist das anwendbare Recht?

Applikationsname:

Erforderlich: Beschreiben Sie die Funktionalität der Applikation.

Textantwort
-

Erhobene Personendaten

Erforderlich: Erfassen Sie alle von der Applikation erhobenen Personendaten inklusive des Zwecks. Kategorisieren Sie wo sinnvoll.

| Kategorie | Attribute | Zweck

Bsp. 1 | Schülerstammdaten | Name, Vorname, Geburtsdatum | Identifikation der Nutzenden

Bsp. 2 | Leistungsdaten | Fähigkeitsniveau, Noten | Steuerung und Bewertung des Lernprozess

Recht & Datenschutz

1. Erforderlich: Geben Sie an wer die für den Datenschutz verantwortliche Person (bspw. Datenschutzbeauftragter DSB) ist.
   Textantwort
2. Erforderlich: Haben Sie Prozesse für datenschutzrechtliche Ansprüche definiert?
   Ja - Beschrieb/Nein - Auskunftsbegehren, Löschbegehren, etc.
3. Erforderlich: Haben Sie eine applikationsspezifische Datenschutzerklärung und ein Impressum?
   Ja - Anhang oder Link/Nein
4. Erforderlich: Haben Sie allgemeine Nutzungsbedingungen definiert?
   Ja - Anhang oder Link/Nein
5. Erforderlich: Nennen Sie alle Server-Standorte wo Daten gespeichert resp. bearbeitet werden. Halten Sie dabei fest, ob es sich um Cloud Systeme oder On-Prem Server handelt.
   Server | Serverstandort | Betreiber |
6. Erforderlich: Wo befindet sich der Hauptsitz des Unternehmens?
   Textantwort

7. Erforderlich: Sofern Subdienstleister* (Auftragsdatenbearbeiter) existieren, wo befinden sich deren Sitz?
   Keine Subdienstleister/
   | Name 1 des Subdienstleister | Standort | ADV vorhanden Ja/Nein
   | Name 2 des Subdienstleister | Standort | ADV vorhanden Ja/Nein
8. Erforderlich: Setzt die Applikation neue Technologien ein?
   Ja - Beschrieb/Nein
   Definition Neue Technologien (Quelle Basel-Landschaft):
   Neue Technologien bergen oft neuartige Risiken für die Rechte und Freiheit der betroffenen Personen. „Neu“ heisst in diesem Falle nicht, dass eine Technologie noch nie eingesetzt wurde. „Neu“ heisst vielmehr, dass mit dem Einsatz einer neuen Technologie in Bezug auf Datenbearbeitungen neue Möglichkeiten oder neue Risiken für die Grundrechte betroffener Personen geschaffen werden. Dabei handelt es sich oft um Technologien bzw. Funktionserweiterungen dazu, welche neue oder zusätzliche Informationen generieren (bspw. Patientenportal, Internet der Dinge, Videoberatung, usw.) oder angepasste Massnahmen für die Gewährleistung der Informationssicherheit erfordern.
9. Erforderlich: Erstellt die Applikation ein Profil der Nutzenden?
   Ja/Nein
   - Bsp. 1: Die Applikation erfasst die Leistungsdaten der Schülerinnen und Schüler innerhalb eines Jahres.
   - Bsp. 2: Die Applikation verwendet Cookies und lokal gespeicherte Daten, um das Nutzungsverhalten der Schülerinnen und Schüler über einen längeren Zeitraum hinweg zu analysieren.
    1. Erforderlich: Werden Cookies, Trackingpixel, Browserfingerprints oder anderweitige Trackingmechanismen eingesetzt und genutzt?
       Ja - *Auflistung und Beschrieb der Trackingmechanismen sowie Angabe des Zwecks und Einstufung (Optional, Erforderlich)*/Nein
    2. Falls Frage 8 mit Ja beantwortet wurde Erforderlich: Werden die Nutzenden darüber informiert, dass ein Profil erstellt wird?
       Ja - Beschrieb/Nein
10. Erforderlich: Ist die Applikation werbefrei?
    Ja/Nein

    1. Wenn nein, ist es möglich die Werbung zu deaktivieren?
       Ja/Nein
11. Erforderlich: Müssen Schüler und Schülerinnen ihre Zustimmung geben, dass ihre Daten bearbeitet werden dürfen?
    Ja/Nein
12. Erforderlich: Wie wird nach Beendigung der Zusammenarbeit mit den Daten der Nutzenden umgegangen?
    Textantwort

    1. Erforderlich: Gibt es eine Möglichkeit bei Beendigung der Zusammenarbeit die Daten der Nutzenden zu exportieren?
       Ja/Nein

13. Erforderlich: Setzt die Applikation Inhalte mit Altersbeschränkung ein?
    Ja/Nein
14. Erforderlich: Welche Drittinhalte aus welchen Quellen setzt die Applikation ein?
    Liste der Drittinhalte inklusive Quellen/ Keine Drittinhalte
    Bspw.
    - Videos: Quelle Youtube
15. Sind Eingabefelder mit Hinweisen versehen, dass keine sensiblen Daten eingegeben werden sollen?
    Ja/Nein
16. Erforderlich: Sind Nutzerdaten pseudonymisiert, anonymisiert oder maskiert?
    Ja - Beschrieb/Nein
17. Erforderlich: Haben Sie weitere Massnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben implementiert?
    Ja - Beschrieb/Nein

KI und Algorithmen

1. Erforderlich: Wird in der Applikation Künstliche Intelligenz oder ein vergleichbarer Algorithmus eingesetzt?
   Ja/Nein
   Definition ähnliche Algorithmen:
   Als vergleichbare Algorithmen gelten Verfahren, die ähnliche Risiken wie Künstliche Intelligenz mit sich bringen. Dazu zählen insbesondere Risiken im Hinblick auf mangelnde Transparenz, eingeschränkte Kontrolle oder potenzielle Voreingenommenheit. Diese Risiken entstehen durch eine datenbasierte Funktionsweise in Kombination mit automatisierten Entscheidungen oder Vorhersagen.
   wenn ja Beschrieb der Funktionsweise

Nur wenn Frage 1 mit Ja beantwortet wurde:

2. Erforderlich: Ist für Nutzende einfach erkennbar wenn sie mit KI oder KI-generierten Inhalten interagieren?
   Ja - Beschrieb/Nein
3. Erforderlich: Trifft die Künstliche Intelligenz oder der Algorithmus eigenständig Entscheidungen, die Auswirkungen auf die Schülerinnen und Schüler haben (vgl. Art. 21 DSG)?
   Ja- Beschrieb/Nein
   Als eigenständige Entscheide gelten in diesem Kontext das automatische Bewerten von Leistungen oder das automatische Steuern des Lernprozess.
   3a und 3b nur wenn Frage 3 mit Ja beantwortet:
   1. Erforderlich: Sind die Entscheidungen erklärbar und nachvollziehbar?
      Ja - Beschrieb/Nein
   2. Erforderlich: Werden die Betroffenen transparent darüber aufgeklärt, dass Entscheidungen über sie durch eine Künstliche Intelligenz oder einen

vergleichbarer Algorithmus erfolgen?
Ja/Nein

4. Erforderlich: Schlägt die Künstliche Intelligenz oder der Algorithmus Entscheidungen zuhanden der Lehrpersonen vor?
   Ja - Beschrieb/Nein
5. Erforderlich: Wie wird die korrekte Funktionsfähigkeit der Künstlichen Intelligenz oder des vergleichbaren Algorithmus sichergestellt?
   Textantwort
6. Erforderlich: Welche Massnahmen werden ergriffen, um sicherzustellen, dass die Resultate von Künstlicher Intelligenz oder algorithmischen Systemen nur ein minimales Diskriminierungsrisiko aufweisen?
   Textantwort
7. Erforderlich: Werden die Daten der Nutzenden verwendet um die eingesetzte KI oder Algorithmus zu verbessern (Training)?
   Ja/Nein

    1. Erforderlich: Werden die Nutzenden darüber informiert, dass ihre Daten zu Trainingszwecken verwendet werden?
       Ja/Nein

Technische Integration der KI oder des Algorithmus

1. Erforderlich: Nennen Sie das oder die verwendeten Modelle.
   Beschrieb: Name, Konfiguration bspw. Anzahl Parameter falls wählbar, Quelle, Hersteller
2. Erforderlich: Wird das Modell selbst betrieben oder via externer Schnittstelle eingebunden?
   selbst betrieben/extern eingebunden
   falls selbst betrieben:
   - Nennen Sie getroffenen Sicherheitsmassnahmen wie bspw. Absicherung der Schnittstelle.
   falls extern:
   - Nennen Sie getroffenen Sicherheitsmassnahmen wie bspw. Absicherung der Schnittstelle.
   - Nennen Sie den Anbieter.

Sicherer Betrieb

Applikationsfokus

1. Erforderlich: Wird eine applikationsspezifische Risikoanalyse in regelmässigen Abständen durchgeführt?
   Ja/Nein
   Wenn ja Beschrieb: Risiken inkl. Massnahmen aufführen

Berechtigungsmanagement

1. Erforderlich: Wie wird das Berechtigungsmanagement umgesetzt und dokumentiert?
   Textantwort
   Beispiel-Konzepte: Least-Privilege, Need-to-Know, RBAC, GBAC
   - Welche Rollen gibt es in der Applikation die von Personen der Schule übernommen werden?
   - Welche Rechte haben diese Rollen?
   - Welche Rollen gibt es in der Applikation die von Personen des Herstellers übernommen werden?
   - Welche Rechte haben diese Rollen?
2. Erforderlich: Wie werden Zugriffsrechte sowie Rollen und Gruppen verwaltet?
   Textantwort
   - Beschreibung wie Benutzerkonten berechtigt, zugeordnet, deaktiviert oder gelöscht werden.
3. Erforderlich: Gibt es eine vordefinierte Benutzerrolle mit den minimal Rechten für neue Nutzer?
   Ja/Nein

Authentifizierung

1. Erforderlich: Wie stellen Sie das sichere Authentifizieren von Nutzenden sicher?
   Textantwort
    1. Erforderlich: Wird eine Multi-Faktor-Authentifizierung unterstützt?
       Ja/Nein
    2. Erforderlich: Werden Single-Sign-On Möglichkeiten angeboten?
       Ja - welche Protokolle/Nein
        1. Optional: Welche Single-Sign-On werden Angeboten?
           Auswahl: Edulog, Switch edu-ID, Microsoft, Google, etc.
    3. Erforderlich: Werden Benutzerkonten in externen Systemen (z. B. Partner- oder Fremdsysteme) benötigt?
       Ja/Nein
    4. Optional: Gibt es eine Begrenzung der Sitzungsdauer (Session-Time)? Falls ja, wie lange bleibt die Sitzung aktiv?
       Textantwort
       - Nennen Sie die Lebensdauer von Access- und Refreshtoken

Passwörter

1. Erforderlich: Welche technischen Vorgaben bezüglich Passwörtern existieren?
   Textantwort
    1. Erforderlich: Werden Passwörter automatisch von der Applikation erstellt?
       Ja/Nein
        1. Erforderlich: Müssen Benutzer das Initialpasswort ändern?
           Ja/Nein

    2. Erforderlich: Wie werden Passwörter an Benutzer kommuniziert?
       Textantwort
    3. Erforderlich: Können Benutzer ihr Passwort ändern?
       Ja/Nein
2. Erforderlich: Wie werden Passwörter gespeichert?
   Textantwort
   Beschreiben Sie das Verfahren (bspw. Hashing, Salting).

Verfügbarkeit

1. Erforderlich: Wie wird sichergestellt, dass für den Betrieb der Applikation stets genügend Ressourcen wie Speicherplatz und Rechenleistung zur Verfügung stehen?
   Textantwort
2. Erforderlich: Welches Service Level Agreement (SLA) garantieren Sie?
   Textantwort
   - Nennen Sie Servicezeiten, Reaktionszeiten, etc.
3. Optional: Ist die Internetanbindung gegen Überlastung geschützt?
   Ja - Beschrieb/Nein
   - Nennen Sie die umgesetzte Massnahmen
4. Optional: Betreiben Sie redundante Systeme?
   Ja/Nein
5. Optional: Sind die Systeme skalierbar und wie schnell können Skalierungsmassnahmen umgesetzt werden?
   Ja - Beschrieb/Nein
   - Nennen Sie die Skalierungsmassnahmen und den Umsetzungszeitraum

Privilegierte Zugänge (Administration)

1. Erforderlich: Sind privilegierte Zugänge immer durch Multi-Faktor-Authentifizierung geschützt?
   Ja/Nein
    1. Erforderlich: Sind privilegierte Zugänge immer persönlich?
       Ja/Nein
2. Erforderlich: Sind privilegierte Zugänge durch weitere Massnahmen geschützt?
   Ja - Beschrieb/Nein
   Bspw. IP-Restriktionen, VPN, Jump Hosts, etc.
3. Optional: Verfügen Administratoren standardmässig über Adminrechte, oder müssen sie diese für administrative Aufgaben jeweils separat aktivieren?
   Auswahl: Administratoren verfügen standardmässig über Adminrechte/ Administratoren müssen diese für administrative Aufgaben jeweils separat aktivieren.
   Textantwort falls “Administratoren müssen diese für administrative Aufgaben jeweils separat aktivieren.“
   Beschrieb des Aktivierungsprozess.

Systemsicherheit

1. Erforderlich: Sind Systeme unterschiedlicher Kunden voneinander getrennt?
   Ja - Beschrieb/Nein
   Beispiel: Mandantentrennung
   - Beschrieb der Umsetzung der Mandantentrennung.
2. Erforderlich: Sind Schnittstellen erfasst, dokumentiert und abgesichert?
   Ja - Auflistung der Schnittstellen inklusive Kurzbeschrieb und Absicherungsart/Nein

Weitere

1. Erforderlich: Sind weitere Massnahmen zum sicheren Betrieb umgesetzt?
   Ja - Beschrieb/Nein

Dienstleisterfokus

Infrastruktur, Prozesse und Verantwortungen

1. Erforderlich: Führen Sie ein Informationssicherheits-Managementsystem (ISMS)?
   Ja/Nein
   Beschrieb - Framework beschreiben bspw. ISO27001, BSI, SOC2
2. Erforderlich: Geben Sie an wer die für die Informationssicherheit verantwortliche Person (Informationssicherheitsbeauftragter ISB) ist.
   Textantwort
    1. Optional: Haben Sie eine Informationssicherheitsrichtlinie erstellt?
       Ja - bitte anhängen/Nein
3. Erforderlich: Verfügen Sie über ein IT-Service Management Ticket Tool?
   Ja - Beschrieb/Nein

    1. Erforderlich: Können Sicherheitsvorfälle gemeldet werden und werden diese entsprechend priorisiert und behandelt?
       Ja - Beschrieb/Nein
       - Beschrieb wie diese gemeldet werden können.
       - Beschrieb wie diese priorisiert und behandelt werden.
    2. Erforderlich: Wie werden Kunden über Schwachstellen oder Sicherheitsvorfälle informiert?
       Textantwort
4. Erforderlich: Verfügen Sie über ein Inventar der eingesetzten Systeme (Software wie auch Hardware)?
   Ja/Nein
5. Erforderlich: Sind physische Sicherheitsmassnahmen wie Zugangskontrollen oder andere Vorkehrungen zum Schutz des Gebäudes vorhanden?
   Textantwort
   Beispiel: Schliesssystem, Alarmanlage, Kameras
6. Erforderlich: Erfolgt eine regelmässige Sensibilisierung der Mitarbeitenden hinsichtlich der Risiken der Informationssicherheit und des Datenschutzes?
   Ja/Nein

7. Erforderlich: Werden die Informationsverarbeitenden Systeme und Prozesse von einer unabhängigen Stelle auditiert?
   Ja - Beschrieb/Nein
   - Umfang, Periodizität des Audits, auditierende Stelle
8. Optional: Sind Informationen (Kundendaten, interne Konzepte) klassifiziert und gekennzeichnet?
   Ja - Beschrieb/Nein
   - Nennen Sie Schutzklassen (intern, vertraulich, etc.)
   - Beschreiben Sie den Vorgang wie die Kennzeichnung erfolgt.
9. Erforderlich: Werden die Arbeitsgeräte durch die Organisation verwaltet?
   Ja/Nein

    1. Erforderlich: Verfügt nur ein eingeschränkter Personenkreis über Adminrechte auf den Arbeitsgeräten?
       Ja/Nein
10. Erforderlich: Gibt es dokumentierte Betriebsabläufe (Standard Operation Procedures SOP) für wiederkehrende Aufgaben?
    Ja/Nein

Patch und Änderungsmanagement

Applikationsfokus

1. Erforderlich: Werden (sicherheitsrelevante) Patches und Änderungen systematisch priorisiert und zeitnah eingespielt?
   Ja - Beschrieb/Nein
    1. Erforderlich: Werden potenzielle Sicherheitslücken systematisch identifiziert und analysiert?
       Ja - Beschrieb/Nein
       - Beispiel: Penetration Tests
2. Erforderlich: Wird sichergestellt, dass nur genehmigte und getestete Software oder Code installiert wird?
   Ja - Beschrieb/Nein

    1. Erforderlich: Werden Wartungen regelmässig geplant, angekündigt und durchgeführt?
       Ja - Beschrieb/Nein

Dienstleisterfokus

1. Optional: Gibt es einen IT-Änderungsmanagement Prozess (Change Management)?
   Ja - Beschrieb/Nein

2. Optional: Wie ist sichergestellt, dass der Änderungsmanagement-Prozess von den Lieferanten* eingehalten wird?
   Textantwort

Schutz vor Schadprogrammen

Applikationsfokus

1. Erforderlich: Wie wird gewährleistet, dass die Applikation sicherheitskonform konfiguriert ist?
   Textantwort
    1. Erforderlich: Werden Massnahmen zur Systemhärtung systematisch umgesetzt (Härtungsprozess)?
       Ja - Beschrieb/Nein
       - Angabe des Standards oder der Richtlinie
2. Erforderlich: Sind weitere Massnahmen zum Schutz vor Schadprogrammen umgesetzt?
   Ja - Beschrieb/Nein

Dienstleisterfokus

1. Erforderlich: Sind alle Systeme (Server und Endgeräte) durch geeignete Massnahmen gegen Malware geschützt?
   Ja - Beschrieb/Nein
2. Optional: Sind Systeme zur Filterung von Webinhalten im Einsatz?
   Ja - Beschrieb/Nein
3. Optional: Werden Massnahmen zur Systemhärtung systematisch umgesetzt (Härtungsprozess)?
   Ja - Beschrieb/Nein
   - Angabe des Standards oder der Richtlinie
4. Optional: Sind weitere Massnahmen zum Schutz vor Schadprogrammen umgesetzt?
   Ja - Beschrieb/Nein

Protokollierung

Applikationsfokus

1. Erforderlich: Werden Systemmeldungen (Logs) gesammelt?
   Ja/Nein
    1. Erforderlich: Wie und wo sind Systemmeldungen (Logs) gespeichert resp. geschützt?
       Textantwort
    2. Erforderlich: Wie lange werden die Systemmeldungen (Logs) aufbewahrt?
       Textantwort

    3. Erforderlich: Wer hat Zugriff auf die Systemmeldungen?
       Textantwort
    4. Erforderlich: Können aus den Logs alle Benutzeraktivitäten nachvollzogen werden?
       Ja/Nein
2. Optional: Werden Systemmeldungen (Logs) systematisch ausgewertet?
3. Erforderlich: Sind die Uhren aller Applikationssysteme synchronisiert?
   Ja/Nein
4. Erforderlich: Sind weitere Massnahmen zur Protokollierung umgesetzt?
   Ja - Beschrieb/Nein

Dienstleisterfokus

1. Optional: Werden Systemmeldungen (Logs) zentral gesammelt und systematisch ausgewertet?
   Ja - Beschrieb/Nein
   Beispiel: Security Information and Event Management (SIEM)

Sichere Software und Tests

Applikationsfokus

1. Erforderlich: Haben Sie Anforderungen und technische Grundsätze für eine sichere System- und Softwarearchitektur definiert?
   Ja - Beschrieb/Nein
2. Erforderlich: Ist sichergestellt, dass die Anforderungen an sichere Softwareentwicklung berücksichtigt sind?
   Ja - Beschrieb/Nein
   Beschrieb: Guideline bspw. nach OWASP ASVS angeben
3. Erforderlich: Ist sichergestellt, dass in Testumgebungen keine Produktivdaten verwendet werden?
   Ja/Nein
4. Erforderlich: Sind Entwicklungs-, Test- und Produktivumgebung logisch voneinander getrennt?
   Ja/Nein
5. Erforderlich: Sind in Testumgebungen sämtliche Schnittstellen abgebildet und getestet?
   Ja/Nein
6. Erforderlich: Ist der Quellcode gegen Manipulation geschützt?
   Ja - Beschrieb/Nein
   - Nennen der Massnahmen
7. Optional: Werden statische Code-Analysen durchgeführt (SAST)?
   Ja - Beschrieb/Nein
8. Optional: Werden Sicherheitstests der Applikation durchgeführt (DAST)?
   Ja - Beschrieb/Nein

9. Erforderlich: Ist sichergestellt, dass die ausgelagerte Entwicklung die Anforderungen an sichere Softwareentwicklung berücksichtigt?
   Ja - Beschrieb/Nein
10. Erforderlich: : Sind weitere Massnahmen für die sichere Softwareentwicklung und Tests umgesetzt?
    Ja - Beschrieb/Nein

Dienstleisterfokus

1. Optional: Ist das Entwicklerteam in den relevanten Bereichen für eine sichere Softwareentwicklung sensibilisiert?
   Ja - Beschrieb/Nein

Lieferantenmanagement

Applikationsfokus

1. Erforderlich: Wie gewährleisten Sie, dass Ihre Lieferanten* angemessene Massnahmen zur Informationssicherheit implementieren und dauerhaft einhalten?
   Textantwort
2. Erforderlich: Haben Sie vertragliche Vereinbarungen zur Einhaltung von Informationssicherheitsmassnahmen mit den Lieferanten* getroffen?
   Ja/Nein
3. Erforderlich: Verfügen die eingesetzten Cloud-Anbieter über international anerkannte Nachweise über implementierte Sicherheitsmassnahmen?
   Ja - Beschrieb/Nein/Nicht anwendbar
4. Erforderlich: Wie ist sichergestellt, dass Lieferanten* nur autorisierten Zugriff auf Nutzerdaten haben?
   Textantwort
5. Optional: Wie stellen Sie sicher, dass die Applikation beim Ausfall eines Cloud-Betreibers weiterhin betriebsfähig ist?
   Textantwort
6. Erforderlich: Sind weitere Massnahmen zur Sicherheit im Umgang mit Lieferanten* umgesetzt?
   Ja - Beschrieb/Nein

Datensicherung

Applikationsfokus

1. Erforderlich: Welche Massnahmen haben Sie getroffen um Datenverlust zu vermeiden?
   Textantwort
   Bspw.

- Nennen Sie die Speicherorte der Datensicherungen.
- Nennen Sie wie diese erstellt werden.
- Nennen Sie die Zeitpunkte und Periodizität der Datensicherungen.

2. Erforderlich: Wie stellen Sie sicher, dass Ihre Datensicherungen im Bedarfsfall zuverlässig wiederhergestellt werden können?
   Textantwort
   Bspw. Backup Restore Tests
   - Beschreiben Sie wie Sie die Ergebnisse dieser Test dokumentieren.
   - Nennen Sie den Intervall der Backup Restore Tests.
3. Erforderlich: Wie sind Datensicherungen gegen Manipulation geschützt?
   Textantwort
4. Erforderlich: Erfolgt eine verschlüsselte Speicherung der Datensicherungen?
   Ja/Nein
5. Erforderlich: Wie ist sichergestellt, dass die Datensicherungs-Routine nicht ausfällt resp. erkannt wird wenn diese ausfällt?
   Textantwort
   Bspw.
   - Beschreiben Sie wie der Ausfall erkannt wird.
   - Beschreiben Sie den Prozess wie auf einen Ausfall reagiert wird.
6. Optional: Sind Datensicherungen in unterschiedlichen Gefahrenzonen gespeichert?
   Ja - Beschrieb/Nein
   Bspw.
   - nicht im selben Gebäude

Detektion und Reaktion

Applikationsfokus

1. Erforderlich: Welche Massnahmen sind für das Management eines Sicherheitsvorfalls implementiert (Security Incident Response Plan)?
   Textantwort
2. Optional: Wie ist die Applikation gegen Verhinderung von Diensten (Denial of Service) geschützt?
   Textantwort
3. Erforderlich: Sind weitere Massnahmen zur Detektion und Reaktion umgesetzt?
   Ja - Beschrieb/Nein

Dienstleisterfokus

1. Erforderlich: Verfügen Sie über einen Notfallplan (Business Continuity Plan)?
   Textantwort
2. Optional: Verfügen Sie über standardisierte Verfahren zur Reaktion auf Sicherheitsvorfälle?
   Textantwort

3. Optional: Welche Massnahmen setzen Sie zur Verhinderung von Social Engineering ein?
   Textantwort
4. Optional: Sammeln Sie proaktiv Informationen über die Bedrohungslage, werten diese aus und reagieren angemessen?
   Textantwort
   Beispiel: Threat Reports, Newsletter, etc.
5. Erforderlich: Haben Sie Prozesse etabliert um kontinuierlich aus Sicherheitsvorfällen zu lernen?
   Ja/Nein
6. Erforderlich: Sind weitere Massnahmen zur Detektion und Reaktion umgesetzt?
   Ja - Beschrieb/Nein

Löschen und Vernichten

Applikationsfokus

1. Erforderlich: Wie stellen Sie sicher, dass nicht mehr benötigte Applikationsdaten – insbesondere personenbezogene Daten ehemaliger Nutzer – vollständig gelöscht werden?
   Textantwort
2. Erforderlich: Sind weitere Massnahmen im Bezug auf Löschen und Vernichten umgesetzt?
   Ja - Beschrieb/Nein

Dienstleisterfokus

1. Optional: Wie stellen Sie sicher, dass auf ausgemusterten Geräten enthaltene Informationen – insbesondere auf Speichermedien wie Festplatten – sicher gelöscht oder die Geräte ordnungsgemäss vernichtet werden?
   Textantwort

Kryptografie

Applikationsfokus

1. Erforderlich: Erfolgt die Kommunikation mit der Applikation verschlüsselt?
   Ja/Nein
    1. Erforderlich: Welche Transport Layer Security wird eingesetzt?
       Textantwort
       Bspw.
       - Nennen Sie den Algorithmus inklusive Schlüssellänge
    2. Erforderlich: Werden für administrative Zwecke genutzte Kommunikationskanäle – beispielsweise SSH – durch geeignete Verschlüsselungs- und

Sicherheitsmechanismen geschützt?
Textantwort

2. Erforderlich: Werden offizielle, vertrauenswürdige Zertifikate verwendet, um die Authentizität von Clients und Servern sicherzustellen?
   Ja/Nein
3. Erforderlich: Sind weitere kryptografische Massnahmen umgesetzt?
   Ja - Beschrieb/Nein

Dienstleisterfokus

1. Erforderlich: Wie wird sichergestellt, dass kryptografische Schlüsselmaterial sicher verwaltet wird?
   Textantwort

Netzwerk

1. Erforderlich: Welche Schutz- und Abwehrmassnahmen des Netzwerks (IDS, IPS, Firewalls, etc.) sind umgesetzt?
   Textantwort
2. Erforderlich: Sind angemessene Netzwerkzonen umgesetzt (Netzwerktrennung)?
   Textantwort
   - Nennen Sie die Zonen und deren Zweck.
3. Erforderlich: Wie stellen Sie die sichere Konfiguration von Netzwerkkomponenten sicher?
   Textantwort
4. Erforderlich: Existiert eine umfassende Dokumentation des Netzwerks?
   Ja/Nein
5. Optional: Werden die Netzwerkkomponenten überwacht?
   Textantwort
   Bspw.
   - Sind diese in der SIEM-Lösung integriert?
6. Erforderlich: Sind weitere Massnahmen zum Schutz des Netzwerks umgesetzt?
   Ja - Beschrieb/Nein

*die Begriffe Subdienstleister, Subakkordant und Lieferant werden Synonym verwendet.

Selbstdeklaration zur Richtigkeit und Vollständigkeit der Angaben

im Rahmen der Risikoabschätzung bei der Nutzung von Software-Dienstleistungen (ISDS)

Die nachfolgende Erklärung ist von der für die Auskunft zuständigen Person des Dienstleistungsanbieters abzugeben:

Erklärung

Ich erkläre hiermit, dass die im Rahmen dieses Fragebogens gemachten Angaben nach bestem Wissen und Gewissen vollständig und wahrheitsgetreu erfolgt sind.

Mir ist bekannt, dass diese Angaben als Grundlage für die Beurteilung von Risiken im Zusammenhang mit dem Einsatz der betreffenden Software im öffentlich-rechtlichen Bildungsbereich dienen. Eine unvollständige oder unzutreffende Beantwortung kann zu falschen Einschätzungen und daraus resultierenden Massnahmen führen.

Ich nehme zur Kenntnis, dass nachträglich bekannt gewordene wesentliche Änderungen oder Unrichtigkeiten umgehend der herausgebenden Stelle mitzuteilen sind.

Ich bin mir bewusst, dass vorsätzlich falsche oder irreführende Angaben rechtliche Konsequenzen nach sich ziehen können. Dies gilt insbesondere im Hinblick auf Art. 251 des Schweizerischen Strafgesetzbuches (Urkundenfälschung).

Ort, Datum:

Name der auskunftsgebenden Person:

Funktion im Unternehmen:

Unterschrift:

Firmenstempel (falls vorhanden):