Qualitäts- und Sicherheitsstandards von eOperations Schweiz

Version vom 18. Dezember 2017

Inhalt

1 Ziel

Alle Services von eOperations Schweiz erfüllen gleiche Basisstandards hinsichtlich Qualität und Sicherheit. Die Standards werden jährlich überprüft und können pro Service mit speziellen Anforderungen ergänzt werden.
Das Ziel ist eine bedarfsgerechte, kostenoptimale Qualität und Sicherheit mit einfachen und übersichtliche Regelungen für Ausschreibungen, Verträge und den betrieblichen Alltag.

2 Allgemeine Qualitätsstandards

- Für Verträge mit externen Dienstleistern gelten die SIK-AGB. Sollte dies ausnahmsweise nicht möglich sein, sollen die Bestimmungen der AGB in Ziffer 7 «Dokumentation», Ziffer 8 «Instruktion», Ziffer 13 «Informationssicherheit, Geheimhaltung und Datenschutz» und soweit passend Ziffer 27 «Wartung von Hardware», Ziffer 28 «Pflege von Software» und Ziffer 29 «Bereitschafts-, Reaktions- und Störungsbehebungszeit» in den Vertrag aufgenommen werden.
- Wo inhaltlich möglich stützen wir uns zur Beschaffung und den Betrieb von Services auf eCH-Standards und arbeiten an deren Weiterentwicklung mit.
- Vorhaben mit Projektcharakter werden nach HERMES geführt.
- Das Servicemanagement von eOperations Schweiz lehnt sich an den ITIL-Standard an.

3 Usability und Accessibility

Die Services von eOperations Schweiz sind nutzerfreundlich gestaltet. Für die Accessibility verwenden wir als Standard die Stufe AA gemäss WCAG 2.0 und lassen unsere Services zertifizieren.

4 Datenschutz- und Sicherheitsstandards

4.1 Generelle Regelungen

- Sofern noch nicht vorhanden erstellt eOperations Schweiz vor der Einführung eines neuen Services eine Schutzbedarfsanalyse und ein Informationssicherheits- und Datenschutzkonzept (ISDS), und setzt das Konzept anschliessend im Betrieb um.
- Schutzbedarfsanalysen und Informationssicherheits- und Datenschutzkonzepte (ISDS) werden spätestens nach fünf Jahren grundsätzlich überprüft.

4.2 Datenschutz

Die Services von eOperations Schweiz fördern den Datenschutz. Sie erfüllen die Vorgaben gemäss Bundesgesetz und Verordnung über den Datenschutz und wo anwendbar gemäss den kantonalen Rechtsgrundlagen. eOperations Schweiz setzt dazu folgende Massnahmen um:

- Bezeichnung einer Datenschutzberaterin / eines Datenschutzberaters für Projekte und für den Betrieb der Services.

- eOperations Schweiz plant, eine Datenschutzzertifizierung zu erlangen, sobald die eigene Rechtspersönlichkeit begründet und das revidierte Datenschutzgesetz in Kraft getreten ist.
- eOperations Schweiz nimmt vor der Einführung eines Services bei Bedarf die Beratung des eigenen Datenschutzberaters und fallweise des/der zuständigen Datenschutzbeauftragten (Bund und/oder Kantone) in Anspruch resp. macht die vorgeschriebenen Meldungen.
- Für jeden Service stimmt eOperations Schweiz mit den involvierten Gemeinwesen die Zuständigkeiten für Informationssicherheits- und Datenschutzbelange ab.
- Wo eOperations Schweiz Auftragsbearbeiterin von Daten ist, holt sie von ihren Kunden eine schriftliche Bestätigung ein, dass diese mit der Bearbeitung ihrer Daten durch Dritte (z.B. Hosting-Dienstleister von eOperations Schweiz) einverstanden sind.

4.3 Sicherheitsstandards

- Für von Dritten zu übernehmende Applikationen und Systeme wird eine Qualitäts- und Sicherheitsprüfung durchgeführt, falls eine solche nicht bereits bestehen sollte (Cyberrisiken, v.a. Intrusion, Analyse des Source Codes und seiner Wartbarkeit, allgemeiner Qualitätsreview).
- Für erweiterte, Service-spezifische Sicherheitsanforderungen stützen wir uns wo sinnvoll und möglich ebenfalls auf etablierte Standards.
- Es erfolgt keine Auslagerung von Prozessen oder Daten ins Ausland.
- Hosting-Dienstleister für Services von eOperations Schweiz (Leistungserbringer von eOperations Schweiz) erfüllen folgende Standards und Anforderungen:

  Private Hosting-Dienstleister

  - ISO 27001 zertifiziert
  - Erfüllen die zusätzlichen Sicherheitsanforderungen gemäss Schutzbedarfsanalyse

  Hosting-Dienstleister des Bundes

  - Erfüllen Anforderungen gemäss IKT-Grundschutz in der Bundesverwaltung
  - Erfüllen die zusätzlichen Sicherheitsanforderungen gemäss Schutzbedarfsanalyse

  Hosting-Dienstleister von Kantonen

  - Erfüllen die Anforderungen gemäss Schutzbedarfsanalyse und den Vorgaben des Kantons
- Auftragnehmer von eOperations Schweiz, die Dienstleistungen in der Applikationsentwicklung resp. –wartung erbringen, erfüllen die in Anhang 1 genannten Ziffern des IKT-Grundschutzes Bund.
- In Vereinbarungen mit externen Dienstleistern integrieren wir das Recht, jederzeit Sicherheitsüberprüfungen durchführen zu können, und die Pflicht der Dienstleister für Applikationsmanagement resp. -Betrieb, die Sicherheitsbedrohungen laufend zu überprüfen und angemessene Gegenmassnahmen zu treffen.

- eOperations Schweiz sorgt dafür, dass die Standards pro Service in denjenigen Teilen des Systems eingehalten werden, für die eOperations Schweiz verantwortlich ist. Für die übrigen Systemelemente gibt eOperations Schweiz der/den verantwortlichen Stelle(n) (z.B. in einem Kanton) bei Bedarf Empfehlungen ab.

5 Nachhaltigkeit

eOperations Schweiz vergibt Aufträge für Leistungen nur an Unternehmen, die:

- die Arbeitsschutzbestimmungen und Arbeitsbedingungen für Arbeitnehmer und Arbeitnehmerinnen einhalten (Nachweis: Selbstdeklaration)
- die Lohngleichheit für Mann und Frau gewährleisten (Nachweis: Selbstdeklaration)
- Hosting-Dienstleistungen CO2-neutral (Nachweis: Selbstdeklaration oder Zertifikat, z.B. myClimate) und energieeffizient (Nachweis: Selbstdeklaration, Power Usage Effectiveness (PUE) mindestens 1,4[1]) erbringen

Für Beschaffungen prüfen wir sowohl monetäre als auch nicht-monetäre Zuschlagskriterien. Für die monetäre Bewertung sind die Kosten massgebend, die während der gesamten Vertragsdauer zu erwarten sind.
Die Nachhaltigkeitskriterien von eOperations Schweiz gehen davon aus, dass die beschafften Dienstleistungen in der Schweiz erbracht werden. Sollte sich dies ändern, sind die Kriterien zu überprüfen.

6 Beschaffungsrecht

Die Beschaffung von Leistungen erfolgen hinsichtlich Form und Intervallen entsprechend den beschaffungsrechtlichen Vorgaben.

Quellen:

- IKT-Grundschutz in der Bundesverwaltung
  https://www.isb.admin.ch/dam/isb_kp/de/dokumente/ikt-vorgaben/sicherheit/Si001-IKT-Grundschutz_V4-0-d.pdf.download.pdf/Si001-IKT-Grundschutz_V4-0-d.pdf
- Allgemeine Geschäftsbedingungen für IKT-Leistungen
  http://www.sik.ch/dok/AGBderSIK-Ausgabe-150101.pdf

[1] s. Rechenzentren in der Schweiz - Energieeffizienz: Stromverbrauch und Effizienzpotenzial, Basel, 2014, https://www.newsd.admin.ch/newsd/message/attachments/36251.pdf, die PUE-Anforderung wird periodisch überprüft und der technologischen Entwicklung angepasst

Anhang 1: Von eOperations angewendete Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf gemäss IKT-Grundschutz in der Bundesverwaltung

(Kapitel 2, S. 8 ff.)

1. Informationssicherheitsleitlinien

Nr. 1.1.1 Dokumentation von Vorgaben und Ziff. 1.1.2 Schutzbedarfsanalysen und ISDS-Konzepte sind fünf Jahre gültig

3. Personalsicherheit und Führungsverantwortung

Nr. 3.1.1, Schulen und Sensibilisieren der Mitarbeitenden

5. Handhabung von Speicher- und Aufzeichnungsmedien

Nr. 5.1 Konzept für den Umgang mit Speichermedien

11. Physische und umgebungsbezogene Sicherheit

Ziff. 11.1 Nr. 11.1.2

12. Betriebssicherheit

Ziff. 12.1 Betriebsverfahren und Verantwortlichkeiten, Nr. 12.1.1, 12.1.2, 12.1.3, 12.1.4

Ziff. 12.2 Schutz vor Schadsoftware (Malware), Nr. 12.2.1, 12.2.3, 12.2.4

Ziff. 12.3 Backup, Nr. 12.3.1, 12.3.2

Ziff. 12.5 Kontrolle von Software im Betrieb, Nr. 12.5.1

Ziff. 12.6 Schwachstellenmanagement, Nr. 12.6.1, 12.6.2

Ziff. 12.7 Auswirkungen von Audits auf Informationssysteme, Nr. 12.7.1, 12.7.2

13. Kommunikationssicherheit

Ziff. 13.1 Management der Netzsicherheit, Nr. 13.1.2, 13.1.3, 13.1.4, 13.1.6, 13.1.7, 13.1.9

14. Beschaffung, Entwicklung und Wartung von Informationssystemen

Ziff. 14.1 Sicherheitsanforderungen an Informationssysteme, Nr. 14.1.2, 14.1.3

Ziff. 14.2 Testdaten, Nr. 14.2.1

16. Umgang mit Informationssicherheitsvorfällen, Nr. 16.1

17. Sicherstellung des Geschäftsbetriebs

Ziff. 17.1 Fortbestand der Informationssicherheit, Nr. 17.1.1