IT-RICHTLINIEN

INHALTSVERZEICHNIS

Du startest gerade ein neues Projekt mit IT-Zusammenhang? Am besten gehst du einmal die Leitfragen in der IT-Richtlinien-App durch!

1. EINLEITUNG / GELTUNGSBEREICH

Diese IT-Richtlinien definieren die Prinzipien und regeln die Prozesse der IT auf der PBS Bundesebene, sie dürfen gerne von den Kantonalverbänden und Abteilungen übernommen und weiterentwickelt werden. Geregelt werden die Punkte Beschaffung, Betrieb und Informationssicherheit sowie die zugehörigen Verantwortlichkeiten. Weiter schaffen sie die Voraussetzungen für eine aktive IT-Community in der PBS.

Dem Dokument ist ein Glossar mit den wichtigsten Fachbegriffen angehängt. Zusätzlich werden die Begriffe «IT-Tools» und «schützenswerte Daten» wie folgt verwendet:

- Als «IT-Tools» werden alle möglichen Arten von Software, Webseiten und IT-Dienstleistungen bezeichnet, die entwickelt, bezogen oder zur Verfügung gestellt werden. Es wird zwischen Standardlösungen und Eigenentwicklungen unterschieden.
- Als «schützenswerte Daten» gelten «Personendaten» und «besonders schützenswerte Personendaten» gemäss geltendem Bundesgesetz über den Datenschutz sowie Daten, welche gemäss Einschätzung der Bundesebene zusätzlich schützenswert sind (wie z.B. Kursrückmeldungen).

2. PRINZIPIEN

1. Die IT-Tools der PBS sind Werkzeuge und nützen in erster Linie dem Pfadibetrieb in den Abteilungen und Kantonalverbänden.
2. Alle Daten gehören der PBS sowie ihren Mitgliedern und müssen angemessen geschützt werden. Daten sollen entkoppelt von den IT-Tools gespeichert und gesichert werden.
3. Nicht schützenswerte Daten dürfen im Sinne von open data veröffentlicht werden.
4. Bestehende Prozesse werden vor der Digitalisierung kritisch hinterfragt und gegebenenfalls angepasst.
5. Jedes IT-Tool hat einen definierten, möglichst begrenzten thematischen Zweck. Dies erleichtert die Ablösung.
6. Für neue IT-Tools soll die Beschaffung von Standardlösungen den Eigenentwicklungen vorgezogen werden. Dabei ist zu prüfen, ob ein bestehender Prozess anzupassen ist.

7. Von der PBS entwickelte, in Auftrag gegebene oder unterstützte IT-Tools werden unter einer open source-Lizenz veröffentlicht.
8. Die IT-Tools sollen barrierefrei gestaltet werden. Bei kleinem Mehraufwand erfolgt dies automatisch, ansonsten werden Kosten und Nutzen abgewogen.
9. Für den Betrieb von IT-Tools auf Bundesebene sollen Dienstleistungen von professionellen Anbietern einer eigenen Infrastruktur im Allgemeinen vorgezogen werden, um die nötige Verfügbarkeit und den Support sicherzustellen.
10. Von der Bundesebene betriebene oder unterstützte IT-Tools sollen über Schnittstellen (APIs) untereinander vernetzt werden können.
    - IT-Tools stellen die von ihnen verwalteten Daten und Dienste so dynamisch und flexibel wie möglich über Schnittstellen zur Verfügung.
    - IT-Tools beziehen fremde Daten über die zur Verfügung gestellten Schnittstellen.
    - Die Schnittstellen und ihre Dokumentation sollen für die Community zur Verfügung stehen, um weitere Entwicklungen zu ermöglichen.
    - Schnittstellen sollen möglichst allgemein gehalten werden und stabil bleiben (d.h. Information bei Änderung, API-Versionierung).
11. Die PBS fördert und unterstützt Ideen, IT-Tools, -Services und -Projekte, welche dem Pfadibetrieb (insbesondere den Abteilungen und Kantonalverbänden) helfen. Dazu wird eine aktive Community angestrebt.
12. Die Bundesebene geht offen und pragmatisch mit IT-Tools um:
    - Synergien zwischen verschiedenen IT-Tools werden nach Möglichkeit genutzt. Falls Mehrspurigkeiten effizienter sind, ist dies aber auch möglich.
    - Für jedes IT-Tool wird individuell über die zweckmässigste Technologie und das eingesetzte Tooling entschieden. Es soll aber, soweit möglich, mit webbasierten und plattformübergreifenden Technologien gearbeitet werden.

3. INFORMATIONSSICHERHEIT

- Die geltenden Datenschutzgesetze der Schweiz werden jederzeit eingehalten.
- Schützenswerte Daten werden deklariert und entsprechend behandelt.
- Eine Datennutzungserklärung liegt pro IT-Tool vor und ist für alle PBS Mitglieder zugänglich.
- Auf schützenswerte Daten darf nur zugegriffen werden, wenn der Nutzen für den Pfadibetrieb gegeben und verhältnismässig ist. Die IT-Tools der PBS stellen diesen Schutz z.B. über Rollen und Zugriffsrechte für Personen und IT-Tools sicher.
- Wenn eine Person eine Berechtigung/Login nicht mehr benötigt, wird diese wieder entzogen.
- Schützenswerte Daten dürfen nur in Ländern gespeichert werden, welche gleichwertige oder strengere Datenschutzgesetze haben wie die Schweiz.
- Für alle relevanten Daten (siehe Kapitel 6.2) wird die Archivierung sichergestellt.
- Externe Zugriffe auf schützenswerte Daten werden durch ein Non-Disclosure Agreement (NDA) geregelt.

- Cyber-Security soll verhältnismässig bei jedem IT-Tool thematisiert und entsprechend implementiert werden. IT-Tools mit Geschäftskritikalität oder schützenswerten Daten müssen gängige Cyber-Security-Standards erfüllen.
- Die PBS sensibilisiert ihre Mitglieder bezüglich des Datenschutzes und möglichen Cyber-Angriffen wie Phishing und Social Engineering, um die Sicherheit schützenswerter Daten sicherzustellen (z.B. Passwortsicherheit, fremde W-LAN, Login auf fremden Geräten, Sichtschutz, aber auch Liegenlassen von Teilnehmendenlisten auf Papier).

4. BESCHAFFUNG UND BETRIEB

Für IT-Tools gelten folgende Grundsätze:

- Standardlösungen: «Wir passen unsere Prozesse der Software an»
- Der langfristige Betrieb ist durch den Einsatz der Standardlösungen gesichert.
- Anpassungen sollen vermieden werden, um die initialen und laufenden Kosten tief zu halten.
- Eigenentwicklungen: «Wir passen die Software unseren Prozessen an»
  - Die langfristige Weiterentwicklung muss bedacht werden, weil es nicht möglich ist, bei der Beschaffung bereits alle Aspekte zu berücksichtigen.
  - Eine grobe Spezifikation des «Minimal Viable Product (MVP)» muss vorab erstellt werden, auf deren Basis der Auftrag zur Entwicklung erteilt werden kann.

4.1 Beschaffungsregeln

- Die Verhältnismässigkeit zwischen Beschaffungs-/Betriebskosten und zu erwartendem Nutzen muss geprüft und festgehalten werden.
- Lifecycle-Überlegungen bis hin zur Abschaltung müssen gemacht und festgehalten werden.
- Sowohl bei Beschaffung von Standardlösungen als auch bei Eigenentwicklungen muss ein zuständiger Product Owner (PO) bestimmt werden.
- Eigenentwicklungen sollen in der Schweiz entwickelt werden. Standardlösungen können auch im Ausland eingekauft werden.
- Die IT-Tools sollen möglichst den CI/CD-Richtlinien der PBS entsprechen.
- Geschäftskritische IT-Tools müssen nach gängigen Standards der Softwareentwicklung inkl. Technologiewahl umgesetzt werden.
- Für geschäftskritische IT-Tools müssen zusätzliche Überlegungen zur Unterstützung der Anwendenden (Support) gemacht werden.
- IT-Tools sollen möglichst ressourcenschonend wartbar sein.

4.2 Betrieb

- Eine SLA/SLO muss anhand der Geschäftskritikalität definiert werden.
- Ein verhältnismässiges Monitoring soll betrieben werden.
- Ein zentrales Lifecycle-Management mit Ablösungs-Roadmap über alle IT-Tools muss geführt werden.
- Geschäftskritische Daten müssen durch ein Backup gesichert werden.
- Damit der Pfadibetrieb nicht unter dem Ausfall (Tool, Daten, Strom nicht verfügbar usw.) von IT-Tools leidet, soll für geschäftskritischen IT-Tools ein Plan B (Business Continuity Management) existieren.
- Der kontinuierliche Betrieb muss sichergestellt werden (z.B. durch kontinuierliches Patching, Monitoring, Pen-Test)

5. COMMUNITY

Die PBS **fördert und unterstützt Ideen, IT-Tools, -Services und -Projekte,** welche dem Pfadibetrieb (insbesondere den Abteilungen und Kantonalverbänden) helfen.

- Alle geförderten IT-Tools müssen unter einer open source-Lizenz veröffentlicht werden, damit möglichst viele davon profitieren.
- Unterstützung kann in verschiedenen Formen erfolgen: Durch Hosting, Source Control, Bereitstellung von unterstützenden IT-Tools, Organisation eines Hackathons, Vermittlung von Ressourcen und Know-how oder durch Beschaffung von finanziellen Mitteln.

Die PBS **bietet eine Anlaufstelle** für die Kantonalverbände und Abteilungen. Sie **fördert einen aktiven Austausch**, holt Ideen ein, bringt Bedürfnisse und Praktiken der Community in Erfahrung und unterhält diese.

- Es werden regelmässige Anlässe organisiert, um diese Ziele zu erreichen, z.B. IT-Konferenz, MiData-Hackathon usw.
- Die Zusammenarbeit wird auch über den Verband hinaus gepflegt, um die Synergien von grösseren Communities (z.B. Hitobito) zu nutzen.

6. ORGANISATION

Um IT-Tools zu managen, setzt die Bundesebene Product Owner (PO) ein. Diese sind auf der Bundesebene eingegliedert. PO müssen keine IT-Spezialisten sein, sondern die Anforderungen des Verbandes an das Produkt kennen, verstehen, weiterentwickeln und verantworten können.

Die Rolle PO wird idealerweise nur von einer Person besetzt, wobei eine Person mehrere PO-Rollen haben kann.

6.1 Verantwortlichkeiten des Product Owner (PO)

- Sammlung und Definition der Anforderungen an das Produkt sowie die Priorisierung der Arbeiten.
- Aufgaben nach PBS Projektleitfaden, falls keine dedizierte Projektleitung vorhanden ist.
- Verantwortung über den ganzen Lifecycle eines IT-Tools.
- Lieferung von Informationen bezüglich IT-Tool-Lifecycle an die ITKom.
- Erarbeitung der Datennutzungserklärung inkl. Zugriffsberechtigungen, wobei insbesondere auf alle schützenswerten Daten eingegangen werden muss.
- Erarbeitung eines Vorschlags zur Klassifikation von schützenswerten Daten des IT-Tools zuhanden der ITKom.
- Im-Auge-Behalten von technischen Schulden und diese transparent machen. Grundsätzlich gilt, dass technische Schulden nur begründet in Kauf genommen und in der Weiterentwicklung abgebaut werden sollen.

6.2 Verantwortlichkeiten der IT-Kommission (ITKom)

- Pflege der IT-Community. Die ITKom übernimmt in diesem Zusammenhang die Rolle eines Katalysators und vernetzt Ideen und Projekte der Pfadi in der Schweiz.
- Unterhaltung der **Unternehmensarchitektur**, mit deren Hilfe die Softwarelandschaft der PBS überblickt und weiterentwickelt werden kann. Die Unternehmensarchitektur sollte pro IT-Tool folgende Punkte beinhalten: Zweck, Services, High-Level-Prozesse, Klassifikation, Technologie-Stack, Lifecycle, Schnittstellen und Verbindungen (zu anderen IT-Tools) und deren Daten-Modelle.
- Zentrales Lifecycle-Management für die langfristige Planung der benötigten Ressourcen.
- Initiale Klassifikation von Geschäftskritikalität, schützenswerten und archivierungspflichtigen Daten pro IT-Tool. Diese Klassifikationen sollen jährlich überprüft werden.
- Regelmässige Überprüfung und bei Bedarf Anpassung der IT-Richtlinien.

6.3 Verantwortlichkeiten der Verbandsleitung (VL)

- Verantwortung für die Überprüfung aller Berechtigungen (z.B. Rollen in der MiData oder generelle Zugriffe auf gewisse IT-Tools) auf Bundesebene pro IT-Tool in einem jeweils sinnvollen, regelmässigen Abstand, mindestens aber jährlich.
- Sicherstellen der Zuweisung eines Product Owner pro IT-Tool.
- Sensibilisierung der Geschäftsstelle und der Bundesebene bezüglich Informationssicherheit und Cyber-Angriffe.
- Sicherstellen der Business Continuity im Zusammenhang mit IT-Tools.

7. GLOSSAR

Barrierefrei
Barrierefreie IT-Tools sind Tools, welche sich auch von Personen mit Einschränkungen oder Beeinträchtigungen, wie z.B. (Farben-)Blindheit, praktisch nutzen lassen.

Business Continuity Management (BCM)
Konzept, wie die Erfüllung der geschäftskritischen Aufgaben des Verbandes oder der unterstützen Prozesse durch Verbands-IT-Tools sichergestellt werden kann, auch wenn z.B. die benötigten IT-Tools oder Lieferanten nicht verfügbar sind. Beispiel: MiData ist nicht verfügbar und das Krisenteam muss eine Telefonnummer ausfindig machen. Die BCM-Lösung für dieses Problem könnte ein Ausdruck der Teilnehmendenliste auf Papier sein.

CI/CD (Corporate Identity / Corporate Design)
Die visuelle Identität einer Organisation inklusive Logo, Design, Farben usw.

Cyber-Security
Unter Cyber-Security versteht man Massnahmen, um Computer, Server, Mobilgeräte, elektronische Systeme, Netzwerke und Daten gegen böswillige Angriffe zu verteidigen.

Datennutzungserklärung
Eine Datennutzungserklärung beschreibt, wie Daten (insbesondere personenbezogene Daten) von einer Organisation verarbeitet werden, das heisst, wie diese Daten gesammelt, genutzt und ob sie an Dritte weitergegeben werden. Darüber hinaus wird oft beschrieben, welche Massnahmen die Organisation ergreift, um die Privatsphäre ihrer Kunden*innen oder Nutzer*innen zu wahren.
https://de.wikipedia.org/wiki/Datenschutzerklärung

Eigenentwicklungen
IT-Tool, welches im Auftrag der Pfadi neu entwickelt wird.

End-of-Life
Zeitpunkt, ab welchem ein IT-Tool nicht mehr betrieben werden kann, beispielsweise wegen veralteter Technologie, fehlenden Updates oder Sicherheitslücken.

Geschäftskritikalität
Beschreibt, wie wichtig ein IT-Tool für den Pfadibetrieb ist.

Hackathon
Freies Treffen von Programmierer*innen, um an einer Software zu arbeiten.

Hosting
Ein Hosting-Provider bietet Infrastruktur im Internet, beispielweise Server- oder Cloud-Infrastruktur.
https://de.wikipedia.org/wiki/Hosting

Lifecycle
Produktlebenszyklus von der Entwicklung, Weiterentwicklung, Wartung bis zur geplanten Abschaltung.

MiData
Mitgliederdatenbank der Pfadibewegung Schweiz. Es handelt sich um das Produkt "hitobito" von Puzzle ITC, einer Open-Source-Webapplikation in der Programmiersprache Ruby-on-Rails.
https://db.scout.ch

Minimal Viable Product (MVP)
Produkt mit der minimalen Menge an Funktionen, die notwendig sind, um die Bedürfnisse für einen Bereich oder Prozess abzudecken.

Monitoring
Die Überwachung und laufende Kontrolle bestimmter Aspekte eines IT-Tools, um Fehler und Probleme frühzeitig zu erkennen.

Non-Disclosure Agreement (NDA)
Ein Geheimhaltungsvertrag, welcher typischerweise durch die Mitarbeitenden von externen Firmen unterzeichnet wird, die aufgrund ihrer Tätigkeit in der Entwicklung oder dem Betrieb der IT-Tools mit schützenswerten Daten (der PBS) in Kontakt kommen.
https://de.wikipedia.org/wiki/Geheimhaltunsvertrag

Open Data
Elektronische Daten, welche frei benutzt, weiterverarbeitet und wiederveröffentlicht werden können.

Open Source, Open Source Software
Software, deren Programmcode unter einer Open-Source-Lizenz (z.B. GPL, MIT License usw.) veröffentlicht ist und an der somit kollaborativ gearbeitet werden kann.

Phishing
Als Phishing bezeichnet man Identitätsdiebstahl (oder den Versuch davon) – häufig in Form von Zugriffsdaten – mittels gefälschter E-Mail, Webseite oder sonstigen Mitteln.
https://de.wikipedia.org/wiki/Phishing

Plattformübergreifend
Software, die auf mehreren Plattformen lauffähig ist.
https://de.wikipedia.org/wiki/Plattformunabh%C3%A4ngigkeit

Product Owner (PO)
Die Person, welche für ein IT-Tool die detaillierten Anforderungen definiert und im sogenannten Backlog priorisiert. Es handelt sich somit um die verantwortliche Person für den Inhalt eines IT-Tools.
https://de.wikipedia.org/wiki/Scrum#Product_Owner

SLA / SLO
Das Service Level Agreement (SLA) definiert die vertraglich garantierte Verfügbarkeit eines Systems und wird typischerweise in Prozent auf das ganze Jahr betrachtet definiert. Das Service Level Objective (SLO) ist dasselbe ohne vertragliche Komponente und entspricht mehr einem Zielwert resp. einem Commitment.
https://de.wikipedia.org/wiki/Service-Level-Agreement

Schnittstellen (APIs)
Application Programming Interface (API) – die technische Möglichkeit, dass ein IT-Tool mit anderen IT-Tools automatisiert Daten austauschen kann.

Social Engineering
Bei **Social Engineering** handelt es sich um ein Verfahren, um sicherheitstechnisch relevante Daten durch das **Ausnutzen menschlichen Verhaltens** zu gewinnen. Dabei wählt der Täter den Menschen als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminellen Absichten in die Tat umzusetzen. Er nutzt dabei menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft, Angst oder Respekt vor Autorität aus, um diese Menschen zu manipulieren.

Source Control
Versionsverwaltung des Source Codes einer Software damit Änderungen und Versionen nachverfolgt werden können.
https://de.wikipedia.org/wiki/Versionsverwaltung

Standardlösung
Existierende Software-Lösung, welche von einer breiten Menge an Organisationen zu einem ähnlichen Zweck eingesetzt wird. Der Einsatz von Standartlösungen führt häufig zu tieferen Kosten in der Anschaffung und im Betrieb und sind mit hoher Wahrscheinlichkeit langlebiger.

Technischen Schulden
Technische Schulden sind technische Umgehungslösungen oder Fehler in der Umsetzung, welche von kurzfristiger Dauer sein sollten, weil sie zusätzliche betriebliche Aufwände, erhöhte Risiken für Ausfälle oder Fehler und/oder die Verhinderung von Funktionalitätserweiterungen nach sich ziehen.
https://de.wikipedia.org/wiki/Technische_Schulden

Tooling
Werkzeuge (Technologie, Programmiersprache, Framework usw.), welche zur Umsetzung eines Projekts eingesetzt werden.