

LIGNES DIRECTRICES IT

TABLE DES MATIÈRES

1. Introduction / Domaine de validité	2
2. Principes	2
3. Sécurité de l'information	3
4. Acquisition et exploitation	4
4.1 Règles d'acquisition	4
4.2 Exploitation	5
5. Communauté	5
6. Organisation	6
6.1 Responsabilité du Product Owner (PO)	6
6.2 Responsabilités de la Commission Informatique (CoIT)	6
6.3 Responsabilités de la maîtrise fédérale (MF)	7
7. Glossaire	7



Tu commences un nouveau projet lié à l'informatique ? Le mieux est de passer en revue les questions directrices de [l'application des lignes directrices IT](#) !

1. INTRODUCTION / DOMAINE DE VALIDITÉ

Ces directives sur l'utilisation des Technologies de l'Information (en anglais IT - Information Technology) définissent les principes et règlent les processus informatiques au niveau fédéral du MSdS. Elles peuvent volontiers être reprises et développées davantage par les associations cantonales et les groupes. Les points régulés sont : l'approvisionnement, le fonctionnement et la sécurité des informations, ainsi que les responsabilités associées. C'est ensuite vous qui mettez en place les conditions préalables pour une communauté informatique active au sein du MSdS.

Un glossaire est annexé au document avec les termes techniques les plus importants. De plus, les termes «outils informatiques» et «données sensibles» sont employés comme suit :

- Le terme "outils informatiques" désigne toute sorte de logiciel, site Web et service sur Internet, qui sont développés, achetés ou mis à disposition. La distinction est faite entre les solutions standard et les développements sur mesure.
- Les "données sensibles" comprennent les "données personnelles" et les "données personnelles particulièrement sensibles" selon la loi fédérale sur la protection des données, ainsi que les données qui nécessitent une protection supplémentaire selon l'évaluation fédérale (par exemple, les retours de cours de formation).



2. PRINCIPES

1. Les outils informatiques du MSdS sont des moyens et servent en première ligne au fonctionnement des groupes scouts et des associations cantonales.
2. Toutes les données appartiennent au MSdS et à ses membres et doivent être correctement protégées. Les données doivent être stockées séparément des outils informatiques et sécurisées.
Les données non protégées peuvent être publiées en tant que open data.
3. Les processus existants sont examinés de manière critique avant la numérisation et adaptés si nécessaire.
4. Chaque outil informatique a un usage thématique défini, le plus limité possible. Cela facilite le remplacement.



5. Pour les nouveaux outils informatique, l'acquisition de solutions standard doit être préférée aux développements sur mesure. Il convient aussi, dans chaque contexte, d'examiner si un processus existe déjà et peut être adapté.
6. Les outils informatiques développés, commandés ou soutenus par le MSdS sont publiés sous une licence open source.
7. Les outils informatiques doivent être conçus sans barrières. S'il y a un petit effort financier supplémentaire, il est fait automatiquement, sinon les coûts et les bénéfices sont évalués.
8. Pour l'exploitation des outils informatiques au niveau fédéral, les services de prestataires professionnels doivent généralement être préférés à une infrastructure en interne afin de garantir la disponibilité et le support nécessaires.
9. Les outils informatiques exploités ou soutenus par le niveau fédéral doivent être reliés entre eux via des **interfaces API**.
 - Les outils informatiques mettent à disposition les données et les services qu'ils gèrent de manière aussi dynamique et flexible que possible via des interfaces.
 - Les outils informatiques obtiennent des données externes via les interfaces fournies.
 - Les interfaces et leur documentation doivent être mises à la disposition de la communauté pour permettre des développements ultérieurs.
 - Les interfaces doivent être aussi générales que possible et rester stables (c'est-à-dire information en cas de modification, versionnement de l'API).
10. Le MSdS promeut et soutient les idées, les outils informatiques, les services et les projets qui aident le scoutisme (en particulier les groupes et les associations cantonales). À cette fin, une communauté active est recherchée.
11. Le niveau fédéral adopte une approche ouverte et pragmatique des outils informatiques :
 - Les synergies entre les différents outils informatiques sont utilisées dans la mesure du possible. Cependant, si une solution multipiste/multivoie est plus efficace, c'est également possible.
 - Pour chaque outil informatique, une décision individuelle est prise sur la technologie la plus appropriée et l'outillage (tooling) utilisé. Toutefois on cherche à utiliser dans la mesure du possible les technologies basées sur le web et multiplateformes.



3. SÉCURITÉ DE L'INFORMATION

- Les lois sur la protection des données en vigueur en Suisse sont respectées à tout moment.
- Les données sensibles sont déclarées et traitées en conséquence.
- Une déclaration d'utilisation des données par outil informatique est disponible et est accessible à tous les membres du MSdS.
- Les données sensibles ne peuvent être consultées que s'il y a un bénéfice proportionné et justifié pour le fonctionnement scout. Les outils informatiques du MSdS assurent cette protection, par exemple via les rôles et les droits d'accès des personnes et des outils informatiques.



- Lorsqu'une personne n'a plus besoin d'une autorisation/login, celle-ci est révoquée.
- Les données sensibles ne peuvent être stockées que dans des pays dont la législation sur la protection des données est équivalente ou plus stricte que celle de la Suisse.
- L'archivage est assuré pour toutes les données pertinentes (voir chapitre 6.2).
- L'accès externe aux données sensibles est régi par un accord de non-divulgence (AND).
- La cybersécurité doit être thématifiée relativement à chaque outil informatique et implémentée en conséquence. Les outils informatiques considérés critiques pour l'activité, ou qui traitent des données sensibles, doivent répondre à des normes communes de cybersécurité.
- Le MSdS sensibilise ses membres à la protection des données et aux éventuelles cyberattaques telles que le phishing et l'ingénierie sociale (Social Engineering), afin d'assurer la sécurité des données sensibles (par exemple, sécurité des mots de passe, W-LAN étranger, login sur des appareils étrangers, protection visuelle, mais aussi laisser traîner des listes de participants sur papier).



4. ACQUISITION ET EXPLOITATION



Les principes suivants s'appliquent aux outils informatiques :

- Solutions standards : « Nous adaptons nos processus au logiciel »
- L'exploitation à long terme est assurée par le recours aux solutions standard.
- Il faut éviter les adaptations afin de maintenir bas les coûts initiaux et permanents.
- Développement sur mesure : « Nous adaptons le logiciel à nos processus »
 - Le développement sur mesure doit être considéré sur le long terme car il n'est pas possible de prendre en compte tous les aspects au stade de l'acquisition.
 - Une spécification approximative du "produit minimal viable (PMV)" produit minimal viable (PMV)" doit être établie à l'avance ; elle sert de base pour passer la commande de développement.

4.1 Règles d'acquisition

- La proportionnalité entre les coûts d'acquisition/d'exploitation et les bénéfices attendus doit être examinée puis respectée.
- Le cycle de vie doit être pris en considération jusqu'à la mise hors service et ces considérations doivent être observées.
- Un Product Owner doit être désigné tant pour l'acquisition de solutions standard que pour les développements sur mesure.
- Les développements sur mesure doivent être développés en Suisse. Les solutions standard peuvent être achetées également à l'étranger.
- Les outils informatiques doivent être conformes, dans la mesure du possible, aux directives CI/CD du MSdS.



- Les outils informatiques critiques pour l'activité doivent être mis en œuvre selon les standards courants de développement de logiciels, y compris dans le choix de la technologie.
- Pour les outils informatique critiques pour l'activité il faut de plus réfléchir aux utilisateurs (soutien technique).
- Les outils informatiques doivent être maintenus les plus économes possibles en ressources.

4.2 Exploitation

- Une SLA/SLO doit être définie en fonction de la criticité pour l'activité.
- Un Monitoring proportionné doit être effectué.
- Pour tous les outils informatiques, il faut une gestion centrale du cycle de vie (Lifecycle Management) avec une feuille de route en cas de remplacement.
- Les données critiques pour l'activité doivent être sécurisées par une sauvegarde.
- Pour éviter que le fonctionnement scout ne souffre d'une défaillance technique (outil, données, électricité non disponible, etc.), un plan B (Business Continuity Management) doit exister pour les outils informatiques critiques pour l'activité.
- Le fonctionnement continu doit être assuré (par ex. par un patching continu, un monitoring, un pen-test)



5. COMMUNAUTÉ



Le MSdS **promeut et soutient les idées, outils, services et projets informatiques** qui aident au fonctionnement scout (en particulier les groupes et les associations cantonales).

- Tous les outils informatiques soutenus doivent être publiés sous une licence Open source pour que le plus grand nombre possible en profite.
- Le soutien peut prendre diverses formes : Hosting, Source Control, mise à disposition d'outils informatiques, organisation d'un Hackathon, mise à disposition de ressources et de savoir-faire ou recherche de fonds.



Le MSdS est un **point de contact** pour les associations cantonales et les groupes. Il favorise un **échange actif**, récolte des idées, s'informe sur les besoins et les pratiques de la communauté et les entretient.

- Des événements réguliers sont organisés pour atteindre ces objectifs, par exemple la conférence sur l'informatique, Hackathon MiData, etc.
- La coopération est également soignée au-delà de l'association afin de profiter des synergies de communautés plus importantes (par exemple Hitobito).





6. ORGANISATION

Pour gérer les outils informatiques, le niveau fédéral utilise des (Product Owner – PO). Ceux-ci sont intégrés au niveau fédéral. Les PO ne doivent pas être des spécialistes en informatique, mais doivent connaître les exigences de l'association pour le produit, les comprendre, les développer et en être responsables. Idéalement, le rôle de PO n'est rempli que par une seule personne, bien qu'une personne puisse avoir plusieurs rôles de PO.

6.1 Responsabilité du Product Owner (PO)

- Récolte et définition des exigences pour le produit ainsi que hiérarchisation du travail.
- Tâches selon le guide de projet MSdS, si aucune gestion de projet spécifique n'est disponible.
- Responsabilité de l'ensemble du cycle de vie d'un outil informatique.
- Transmission des informations concernant le cycle de vie des outils informatiques à la CoIT.
- Élaboration de la politique de confidentialité, y compris les autorisations d'accès, qui doit couvrir en particulier toutes les données sensibles.
- Elaboration d'une proposition de classification des données sensibles de l'outil informatique à l'attention de la CoIT.
- Garder un œil sur les dettes techniques et les rendre transparentes. En règle générale, les dettes techniques ne doivent être acceptées que sur justification et réduites dans le cadre d'un développement ultérieur.

6.2 Responsabilités de la Commission Informatique (CoIT)

- Entretien de la communauté informatique. Dans ce contexte, la CoIT joue le rôle de catalyseur et met en réseau les idées et les projets du scoutisme en Suisse.
- Maintien de l'**architecture d'entreprise**, qui peut être utilisée pour avoir une vue d'ensemble et développer le paysage logiciel du MSdS. L'architecture d'entreprise doit inclure les éléments suivants par outil informatique : Objectif, services, processus de haut niveau, classification, pile technologique, cycle de vie, interfaces et connexions (avec d'autres outils informatiques) et leurs modèles de données.
- Gestion centrale du cycle de vie pour une planification à long terme des ressources nécessaires.
- Classification initiale de la criticité pour l'activité, des données à protéger et des données à archiver par outil informatique. Ces classifications doivent être revues chaque année.
- Révision régulière et, si nécessaire, ajustement des directives informatiques.



6.3 Responsabilités de la maîtrise fédérale (MF)

- Responsabilité de la vérification pour chaque outil informatique de toutes les autorisations (par exemple, les rôles dans MiData ou l'accès général à certains outils informatiques) au niveau fédéral à un intervalle régulier raisonnable, mais au moins une fois par an.
- Assurer l'attribution d'un Product Owner par outil informatique.
- Sensibiliser le secrétariat général et le niveau fédéral à la sécurité de l'information et aux cyber-attaques.
- Assurer la continuité des activités (Business Continuity) liées aux outils informatiques.



7. GLOSSAIRE

Sans barrière

Les outils informatiques sans barrières sont des outils qui peuvent être utilisés de manière pratique par des personnes présentant des limitations ou des handicaps, tels que le daltonisme.

Business Continuity Management (BCM)

Concept qui précise comment les tâches critiques pour l'association ou les processus pris en charge par les outils informatiques de l'association peuvent être assurés, même si, p. ex., les outils informatiques ou les fournisseurs requis ne sont pas disponibles. Exemple : MiData n'est pas disponible et l'équipe de crise doit trouver un numéro de téléphone. La solution BCM pour ce problème pourrait être une impression papier de la liste des participants-es.

CI/CD (Corporate identity / Corporate design)

L'identité visuelle d'une organisation, y compris le logo, le design, les couleurs, etc.

Cybersécurité

La cybersécurité désigne les mesures visant à défendre les ordinateurs, les serveurs, les dispositifs mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes.

Politique de confidentialité

Une politique de confidentialité décrit la manière dont les données (notamment les données à caractère personnel) sont traitées par une organisation, c'est-à-dire comment ces données sont collectées, utilisées et si elles sont transmises à des tiers. En outre, elle décrit souvent les mesures prises par l'organisation pour protéger la vie privée de ses client·e·s ou utilisateur·rice·s. https://fr.wikipedia.org/wiki/Politique_de_confidentialité

Développements sur mesure

Outil informatique nouvellement développé pour le compte des scouts.



End-of-life

Point à partir duquel un outil informatique ne peut plus être utilisé, par exemple en raison d'une technologie dépassée, d'un manque de mises à jour ou de lacunes en matière de sécurité.

Criticité de l'activité

Décrit l'importance d'un outil informatique pour le fonctionnement du scoutisme.

Hackathon

Réunion libre de programmeur-euse-s pour travailler sur un logiciel.

Hosting – Fournisseur d'hébergement

Un fournisseur d'hébergement offre une infrastructure sur l'internet, par exemple des serveurs ou une infrastructure cloud. https://fr.wikipedia.org/wiki/Hébergeur_web

Lifecycle – Cycle de vie

Cycle de vie du produit depuis le développement, l'amélioration, la maintenance jusqu'à l'arrêt planifié.

MiData

Base de données des membres du mouvement scout suisse. Il s'agit du produit "hitobito" de Puzzle ITC, une application web open source dans le langage de programmation Ruby-on-Rails.

<https://db.scout.ch>

Minimal Viable Product (MVP)

Produit comportant le minimum de fonctionnalités nécessaires pour couvrir les besoins d'un domaine ou d'un processus.

Monitoring

La surveillance et le contrôle courant de certains aspects d'un outil informatique afin de détecter les erreurs et les problèmes à un stade précoce.

Non-disclosure agreement (NDA)

Un accord de non-divulgence généralement signé par les employés d'entreprises externes qui entrent en contact avec des données sensibles (du MSdS) en raison de leur travail de développement ou d'exploitation des outils informatiques.

https://fr.wikipedia.org/wiki/Accord_de_non-divulgence



Open Data

Données électroniques qui peuvent être librement utilisées, traitées et republiées.

Open Source, Open Source Software

Logiciel dont le code est publié sous une licence open source (par exemple, GPL, MIT License, etc.) et sur lequel il est donc possible de travailler de manière collaborative.

Phishing - Hameçonnage

Le phishing est le terme utilisé pour décrire l'usurpation d'identité (ou la tentative d'usurpation d'identité) - souvent sous la forme de données d'accès - au moyen d'un faux courriel, site web ou autre.

<https://fr.wikipedia.org/wiki/Hameçonnage>

Multiplateforme

Un logiciel qui peut fonctionner sur plusieurs plateformes.

https://fr.wikipedia.org/wiki/Logiciel_multiplateforme

Product Owner (PO)

La personne qui définit les exigences détaillées d'un outil informatique et les classe par ordre de priorité dans ce qu'on appelle le backlog. Il s'agit donc de la personne responsable du contenu d'un outil informatique.

[https://fr.wikipedia.org/wiki/Scrum_\(développement\)](https://fr.wikipedia.org/wiki/Scrum_(développement))

SLA / SLO

L'accord de niveau de service (Service Level Agreement - SLA) définit la disponibilité contractuellement garantie d'un système et est généralement défini comme un pourcentage sur l'ensemble de l'année. L'objectif de niveau de service (Service Level Objective - SLO) est le même sans composante contractuelle et correspond davantage à une valeur cible ou à un engagement.

https://fr.wikipedia.org/wiki/Service-level_agreement

Interfaces (APIs)

Interface de programmation d'applications (API) - la possibilité technique pour un outil informatique d'échanger automatiquement des données avec d'autres outils informatiques.

Ingénierie sociale – Social Engineering

L'ingénierie sociale est une méthode permettant d'obtenir des données relatives à la sécurité en exploitant le comportement humain. L'auteur choisit des personnes comme maillon supposé le plus faible de la chaîne de sécurité afin de mettre en pratique ses intentions criminelles. Il exploite les caractéristiques humaines telles que la confiance, la servabilité, la peur ou le respect de l'autorité afin de manipuler ces personnes.

Source Control – Contrôle des sources

Gestion des versions du code source d'un logiciel afin de pouvoir suivre les modifications et les versions.

https://fr.wikipedia.org/wiki/Gestion_de_versions



Solution standard

Solution logicielle existante qui est utilisée par un grand nombre d'organisations dans un but similaire. L'utilisation de solutions standard permet souvent de réduire les coûts d'acquisition et d'exploitation et sont très probablement plus durable.

Dettes techniques

La dette technique est constituée de solutions techniques de contournement ou d'erreurs de mise en œuvre qui devraient être de courte durée, car elles impliquent un effort opérationnel supplémentaire, un risque accru d'échec ou d'erreurs, et/ou l'empêchement de l'élargissement des fonctionnalités.

https://fr.wikipedia.org/wiki/Dette_technique

Tooling - outillage

Les outils (technologie, langage de programmation, cadre de travail, etc.) qui sont utilisés pour mettre en œuvre un projet.

