Concept SIPD

En-tête \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Désignation du projet informatique
* Service communal compétent
* Responsable du projet (nom et coordonnées)
* Version/date (contrôle des versions)
* Visa du mandant

1. Données relatives au projet

(Il est aussi possible de se référer à des documents existants.)

* Description détaillée du ou des processus qui doit ou doivent être soutenus au moyen de la solution informatique prévue.
* Description des interfaces de données et de résultats, en particulier des accès en ligne pour les tiers (procédure d’appel)
* Description de la solution ou des solutions informatiques à disposition

2. Protection des données

* Enumération des bases légales déterminantes pour le ou les processus, en particulier celles qui autorisent les accès en ligne de tiers (procédure d’appel), voir la liste de contrôle sur l’évaluation de la protection des données
* Le cas échéant, explications sur les possibilités de parvenir à créer ou à compléter les bases légales absentes ou insuffisantes d’ici la mise en service du système
* Archivage et destruction des données
* Description des procédures à même de garantir les droits à la protection des données des personnes concernées (information/consultation, rectification et blocage).
* Concept des droits d’utilisateur du système
* Remise du fichier ou des fichiers à l’autorité de surveillance de la protection des données (sous forme de pièce jointe).

3. Sécurité de l’information

Protection de base

Il s’agit d’exposer, au moyen de la liste de contrôle sur la protection de base[[1]](#footnote-1), les risques fondamentaux liés à l’infrastructure et à la gestion des données et des utilisateurs ainsi que les mesures qui ont été prises en vue de garantir la protection de base.

Besoin de protection accru / protection de l’application

Il convient ensuite de préciser s’il existe un besoin de protection accru, dépassant la protection de base, et quelles mesures sont prises à cet égard. L’évaluation des risques fournit des indices utiles.

L’évaluation des risques pour une application comprend les points suivants:

* 1. Une *analyse de la valeur de l’information* révèle quels dommages matériels naîtraient en cas de perte partielle ou totale des informations.
  2. Une *analyse des menaces* permet de déterminer qui, le cas échéant, pourrait avoir un intérêt à un accès (illégal) aux informations et quel potentiel criminel une utilisation abusive des informations pourrait représenter.
  3. Une *classification* fournit le rang auquel l’application se situe du point de vue de la disponibilité et de la confidentialité des données.

4. Mesures

Liste des mesures techniques et organisationnelles nécessaires jusqu’à la mise en service. A cet égard, sont obligatoires:

* un concept des droits d’utilisateur du système;
* des mesures de protection de base concernant la sécurité de l’information, conformément à la liste de contrôle relative à la protection de base;
* des mesures qui, le cas échéant, couvrent un besoin de protection accru;
* des indications sur la mise en œuvre des mesures d’ici l’introduction du système (plan de mesures).

1. La rédaction de cette liste suppose l’utilisation d’une norme reconnue [p. ex.: Bonnes pratiques d’ISO 27000 (www.iso.org/iso/fr/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=41933) ou Directives du Conseil de l’informatique de la Confédération (CI) (<https://www.isb.admin.ch/isb/fr/home/themen/sicherheit.html>) [↑](#footnote-ref-1)