

**Exemple de politique de sécurité**

**Introduction**

Le bon fonctionnement du CPAS dépend en grande partie de l’information qui est traitée, produite et communiquée. Cette information est très vaste et peut exister sur divers supports : papier et digital portable ou non.

On trouve dans ces supports de l’information concernant le personnel du CPAS ainsi que tous les bénéficiaires des droits légaux. Cette information est confidentielle et doit la rester.

Comme toute autre institution fédérale et régionale, le CPAS doit faire face à une multitude de risques et menaces pouvant porter atteinte à la confidentialité, l’intégrité et la disponibilité de son information. Ces menaces, en constante évolution, comprennent, entre autres, le vol d’identité et d’information confidentielle, la fraude le vol de propriété intellectuelle, l’utilisation, la divulgation et la destruction d’information, les défaillances techniques, les événements naturels et l’erreur humaine.

Par ailleurs, le CPAS est soumis à plusieurs exigences légales, fédérales et régionales, découlant de ses missions et liées à la sécurité de l’information. Le respect de ces exigences et le lien de confiance qui existent envers les membres du personnel et les bénéficiaires sont essentiels au maintien de sa réputation et de son bon fonctionnement.

Ce n’est qu’à cette condition que le CPAS pourra mener ses missions de façon correcte et dans le respect des normes et lois à respecter.

Dans le domaine de la sécurité sociale, la sécurité de l'information se définit comme étant la stratégie, les règles, les procédures et les moyens de protection de tout type d'information tant dans les systèmes de transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information. (Cfr. Arrêté royal du 17 mars 2013 relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l’organisation d’un intégrateur de services fédéral).

**Objectifs**

Cette politique constitue un des éléments clés permettant d’assurer la réalisation de la mission et des objectifs du CPAS afin de maintenir sa réputation et de se conformer aux exigences légales, réglementaires et contractuelles applicables.

L’objectif principal de cette politique est de communiquer la détermination et l’engagement du Conseil de l’Action sociale / du Bureau permanent de gérer et de soutenir la gestion des risques liés à la sécurité de l’information. L’approche préconisée vise l’identification des intervenants et la définition de leurs rôles, la sensibilisation des utilisateurs aux risques et la conception et l’implantation de mesures qui assurent efficacement la sécurité des actifs informationnels.

Les objectifs suivants sont également visés:

1. le respect de la vie privée et des obligations légales se rapportant au traitement des données à caractère personnelle et sociale,

2. la conformité aux normes minimales fixées par le comité sectoriel de sécurité sociale et de la santé dans le cadre du traitement des données précitées,

3. l’inventaire des ressources et leur sécurisation conforme à la classification des données,

4. la mise en œuvre d’un processus de gestion de risques selon une méthode documentée pour l’ensemble des processus critiques,

5. la disponibilité, l’intégrité et la confidentialité des informations,

6. une amélioration continue de la sécurité de l’information,

7. l’intégration des exigences sécuritaires requises dans une convention lorsque l’on fait appel à des sous-traitants ou à des fournisseurs.

**Portée**

La sécurité de l’information est l’affaire de tous. Cette politique s’applique à tous les utilisateurs des ressources informationnelles du CPAS qui incluent, entre autres, le/la Président()e, les membres du Conseil de l’Action sociale, le/la Directeur(trice) général(e), le conseiller en sécurité et les membres du personnel.

Les sous-traitants, fournisseurs et partenaires du CPAS seront liés au CPAS par une clause de confidentialité.

Cette politique s’applique à toute information détenue par le CPAS ou à laquelle le CPAS a accès, que cette information soit conservée ou non sur un support quelconque.

**Responsabilités**

Chaque personne ou service est imputable de la gestion des risques à la sécurité de l’information en sa qualité de propriétaire de l’information. Cette imputabilité s’applique aux actifs informationnels, aux processus et aux systèmes sous leur responsabilité ou leur contrôle, incluant ceux délégués à un tiers.

**Conformité**

La gestion des risques à la sécurité de l’information est faite en conformité avec les exigences légales,

réglementaires et contractuelles applicables ainsi qu’avec les politiques et règlements fédéraux et régionaux.

**Sensibilisation**

Des mesures adéquates sont mise en place pour sensibiliser et faire participer activement tous les utilisateurs et intervenants à la protection de l’actif informationnel du CPAS et favoriser une utilisation responsable des ressources.

Rôles et responsabilités

La présente politique et son application relèvent de différents intervenants à qui les mandats suivants sont attribués :

**Conseil de l’Action sociale**

- approuve la politique ainsi que ses mises à jour;

- supervise le processus de gestion des risques à la sécurité de l’information, par l’intermédiaire du conseiller en sécurité et du responsable de la gestion journalière.

**Bureau permanent**

- recommande au Conseil de l’Action sociale l’adoption de la politique ainsi que ses mises à jour;

- supervise le processus de gestion des risques à la sécurité de l’information et l’application de la politique;

- rend compte, au besoin, à ….

**Direction**

- propose la politique de sécurité ainsi que ses mises à jour et recommande au Bureau permanent son adoption par …

- ’assure de l’application de la politique par le Conseiller en sécurité de l’information;

- s’assure que le conseiller en sécurité de l’information dispose des ressources financières et logistiques appropriées.

**Conseiller à la sécurité de l’information**

Conformément à l’AR du 12/08/93, le conseiller en sécurité de l’information a les responsabilités suivantes :

* le conseiller en sécurité de l’information a une mission d’avis, de stimulation, de documentation et de contrôle ;
* le conseiller en sécurité de l’information conseille le responsable de la gestion journalière de son CPAS, à la demande de celui-ci ou de sa propre initiative, au sujet de tous les aspects de la sécurité de l’information. Sauf si les risques ne sont pas suffisamment importants, les avis s’expriment par écrit et sont motivés. Dans le délai requis par les circonstances, mais avec un maximum de trois mois, le responsable de la gestion journalière décide de suivre ou non les avis et informe le service chargé de la sécurité de la décision adoptée. Si la décision déroge à un avis exprimé par écrit, elle doit être communiquée de façon écrite et motivée.
* le conseiller en sécurité de l’information promeut le respect des règles de sécurité imposées par une disposition ou règlementaire ou en vertu d’une telle disposition, ainsi que l’adoption, par les personnes employées dans l’institution, d’un comportement favorisant la sécurité ;
* le conseiller en sécurité de l’information rassemble la documentation utile à ce sujet ;
* le conseiller en sécurité de l’information veille au respect, dans le CPAS, des règles de sécurité imposées par une disposition légale ou règlementaire ou en vertu d’une telle disposition. Toutes les infractions constatées sont communiquées par écrit et exclusivement au responsable de la gestion journalière de l’institution, accompagnées des avis nécessaires en vue d’éviter de telles infractions à l’avenir ;
* le conseiller en sécurité de l’information est placé sous l’autorité fonctionnelle directe du responsable de la gestion journalière du CPAS. Il travaille en étroite collaboration avec les services qui requièrent, ou peuvent requérir, son intervention, en particulier avec le service informatique et le service de sécurité d’hygiène et d’embellissement des lieux de travail de l’institution ;
* conseiller en sécurité de l’information doit disposer d’une connaissance suffisante de la structure informatique du CPAS ainsi que de la sécurité de l’information. Il doit en permanence tenir cette connaissance à jour ;
* le conseiller en sécurité de l’information rédige un projet de plan de sécurité pour une durée de trois ans, à l’attention du responsable de la gestion journalière, en spécifiant sur base annuelle les moyens nécessaires à la réalisation du plan. Ce projet est révisé au moins annuellement et adapté si nécessaire. Le projet de plan de sécurité est considéré comme un avis,
* le conseiller en sécurité de l’information rédige un rapport annuel à l’attention du responsable de la gestion journalière de l’institution.

Ce rapport comprend au moins :

1° un aperçu général de la situation en matière de sécurité, de l’évolution au cours de l’année écoulée et des objectifs qui doivent encore être atteints;

2° un résumé des avis écrits, transmis au responsable de la gestion journalière et la suite qui y a été réservée;

3° un aperçu des travaux exécutés par le service chargé de la sécurité de l’information;

4° un relevé des résultats des contrôles effectués par le service chargé de la sécurité de l’information, reprenant tous les incidents qui ont été constatés et qui étaient de nature à compromettre la sécurité de l’information de l’institution ou du réseau;

5° un relevé des campagnes menées en vue de favoriser la sécurité;

6° un aperçu de toutes les formations suivies et prévues.

7 les missions du conseiller en sécurité de l’information telles que définies l’AR se rapportent également aux données sociales à caractère personnel conservées, traitées ou échangées par l’intermédiaire de tiers pour le compte de l’institution concernée.

**L’utilisateur**

Il prend connaissance et adhère aux politiques, règlements, codes de conduite et autres directives

pertinentes du CPAS touchant à la sécurité de l’information qui le concernent.

Il s’informe et participe activement à la mise en œuvre de la politique et il utilise les actifs informationnels en se limitant aux fins auxquelles ils sont destinés et à l’intérieur des accès qui lui sont accordés.

Définitions

Pour l’application de la présente politique.

**Actif informationnel**

L’information elle-même, peu importe son support, ainsi que les systèmes utilisés pour son traitement, utilisation, stockage, conservation et communication. La perte, le vol ou la destruction d’un tel actif pourrait causer un préjudice au CPAS. Des exemples d’actifs informationnels sont le dossier physique et/ou informatique du bénéficiaire, les archives et les dossiers des membres du personnel*.*

**Cycle de vie**

Les cycles de vie sont déterminés par les archivistes du royaume mais la conservation des logs des utilisateurs est de 10 ans au moins.

**Risques liés à la sécurité de l’information**

Est considéré comme risque tout événement, comportant un degré d’incertitude, qui pourrait porter atteinte à la confidentialité, l’intégrité ou la disponibilité de l’information et causer un préjudice au CPAS.

**Principes de sécurité, normes et exigences de sécurité.**

Les principes de sécurité suivis sont les suivants :

* confidentialité,
* intégrité,
* disponibilité,
* auditabilité.

Par ailleurs, les normes et exigences particulièrement importantes pour le respect de la sécurité de l’information sont :

* l’AR du 12/08/93 et ses adaptations,
* les normes minimales de sécurité de la BCSS,
* les lignes directrices de la Commission de la vie privée ,
* la loi sur le respect de la vie privée.

4. Cadre législatif et réglementaire.

Les références utilisées sont:

- les normes minimales 2015 de la BCSS.

- les normes ISO 27001, ISO 27002:2013 et ISO 2700.

- " Harmonisation des fonctions de sécurité de l’information " proposition du comité BELNIS ;

- l’AR du 12/08/93 (<https://www.ksz-bcss.fgov.be/fr/bcss/anchorpage/content/websites/belgium/legislation/legislation_03/legislation_03_01.html>);

- la politique de sécurité de l’information de la BCSS (<https://www.ksz-bcss.fgov.be/fr/bcss/page/content/websites/belgium/security/security_04/security_04_02.html>);

- les recommandations de la Commission de la vie privée : <https://www.privacycommission.be/fr>