Union des Villes et
Communes de Wallonie
asbl

Fédération des CPAS

Exemple de politique formelle de sécurité pour les CPAS

Elaboré par Laurence Pirlot, Présidente de la Commission BCSS/MediPrima de la Fédération des CPAS, Conseiller en sécurité du CPAS de Huy.
En collaboration avec Judith Duchêne, Conseiller à la Fédération des CPAS.

Contacts : Laurence Pirlot (CPAS de Huy) - laurence.pirlot@cpashuy.be
Judith Duchêne (Fédération des CPAS) - jdu@uvcw.be

EXEMPLE DE POLITIQUE FORMELLE DE SECURITE POUR LES CPAS[1]

1. CONTEXTE ET ENGAGEMENT DU CONSEIL DE L'ACTION SOCIALE

Le CPAS de *[XXX]* s'appuie sur son personnel et dispose de ses biens afin de fournir les services qui aident les personnes dans une situation de nécessité.

Le CPAS doit gérer ses ressources avec une diligence raisonnable et conformément à la législation.

Il prend les mesures appropriées pour sauvegarder ses ressources de tout préjudice.

Les menaces qui peuvent créer un préjudice au personnel et aux biens du CPAS sont la violence, le vol, la fraude, le vandalisme, l'incendie, les catastrophes naturelles, les défaillances techniques et les dommages fortuits.

Les attaques informatiques et les actes malveillants par internet comptent parmi ces menaces. Ils sont de plus en plus fréquents et peuvent nuire gravement tant à l'infrastructure informatique qu'au bon fonctionnement du CPAS.

Il s'agit donc de définir et de faire appliquer une politique de sécurité au sein du CPAS de *[XXX]* pour se prémunir au mieux de ces menaces et minimiser tout préjudice éventuel.

Il est par ailleurs évident que le bon fonctionnement du CPAS repose grandement sur les technologies de l'information pour la bonne exécution de ses missions.

Par conséquent, cette politique se doit d'accorder une importance particulière mais non exclusive à la surveillance des opérations électroniques dans le cadre des Normes minimales de Sécurité éditées par la Banque Carrefour de la Sécurité sociale (BCSS).

Cette politique est complémentaire aux politiques existantes tant au niveau fédéral que régional et communautaire notamment pour la gestion des ressources humaines, des langues, des régions, du matériel et des ressources du CPAS. Le respect de ces exigences et le lien de confiance qui existent envers les membres du personnel et les bénéficiaires sont essentiels au bon fonctionnement du CPAS. Ce n'est qu'à cette condition que le CPAS pourra mener ses missions légales dans le respect des normes et loi à respecter.

Dans l'Arrêté royal du 12 août 1993 organisant la sécurité de l'information dans les institutions de sécurité sociale, la « sécurité de l'information » est définie comme : « *la prévention et la réparation rapide et efficiente des dommages aux données sociales et des violations illégitimes de la vie privée des intéressés* ».

Le Conseil de l'action sociale s'engage dès lors à soutenir toutes les actions qui s'inscrivent dans cette politique de sécurité et à mettre à disposition les moyens humains, matériels, environnementaux et financiers nécessaires pour l'appliquer efficacement et durablement.

---

[1] Elaboré notamment sur base des sources suivantes :
- SPP Intégration sociale, *Exemple de politique de sécurité 2016*. V. https://www.mi-is.be/fr/outils-cpas/securite-dinformation [consultation le 30.11.2016].
- Avis des Belgian Senior Consultants Wallonie.

À cette fin, un plan pluriannuel en matière de sécurité sera présenté au Conseil, chaque année, à l'initiative du Conseiller en sécurité et un budget spécifique devra être adopté en conséquence.

2. OBJECTIFS DE LA POLITIQUE DE SÉCURITÉ

Cette politique de sécurité constitue un des éléments clés permettant d'assurer la réalisation des missions et objectifs du CPAS et de se conformer aux exigences légales, réglementaires et contractuelles applicables.

L'objectif de cette Politique de Sécurité et de l'engagement du Conseil est triple :

- assurer la sauvegarde du personnel, des biens et des ressources du CPAS afin d'en garantir un fonctionnement fiable, professionnel et permanent ;

- garantir la confidentialité et la protection de la vie privée des personnes faisant appel à ses services ;

- instaurer une culture de la sécurité auprès des membres du Conseil de l'action sociale et le personnel du CPAS en l'informant des normes de sécurité.

3. PORTÉE DE LA POLITIQUE DE SÉCURITÉ

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, qu'elle soit conservée ou non sur un support quelconque.

4. APERÇU DES OBLIGATIONS LÉGALES ET RÉGLEMENTAIRES

Rappel des documents légaux et réglementaires essentiels d'application dans la gestion d'un CPAS.

- Loi organique du 8 juillet 1976 des CPAS.
- Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.
- Arrêté royal du 12 août 1993 organisant la **sécurité de l'information** dans les institutions de sécurité sociale, moniteur belge du 21 août 1993 modifié par l'Arrêté royal du 8 octobre

1998 (moniteur belge du 24 décembre 1998). Voir à ce propos les normes minimales de sécurité à respecter par les Institutions Sociale en vue de leur connexion au réseau de la Banque Carrefour de la Sécurité Sociale.
- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de **données à caractère personnel**.
- Loi du 8 août 1983 organisant un **Registre national** des personnes physiques.
- Arrêté royal du 4 mars 2005 relatif à l'extension du réseau de la sécurité sociale aux centres publics d'aide sociale, en ce qui concerne leurs missions relatives au droit à l'aide sociale, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité Sociale.
- Loi du 30 juin 1994 sur la protection de la vie privée contre les écoutes, la prise de **connaissance et l'enregistrement de communications et de télécommunications privées**.
- Loi du 31 mars 1991 portant **réforme de certaines entreprises publiques** économiques.
- Arrêté royal du 4 février 1997 organisant la **communication des données entre institutions de sécurité sociale.**
- Loi du 28 novembre 2000 en matière de **criminalité informatique**.
- Loi du 30 juin 1994 sur le **droit d'auteur et les droits voisins**.
- Loi du 30 juin 1994 transposant la directive européenne du 14 mai 1991 sur la **protection juridique des programmes** d'ordinateur.
- Loi du 31 août 1998 transposant la directive européenne du 11 mars 1996 sur la **protection juridique des bases de données**.
- Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.
- Arrêté royal du 9 juillet 2001 réglementant la destruction des banques de données de la Banque Carrefour de la Sécurité Sociale et des banques de données sociales ou des données sociales à caractère personnel y conservées, en exécution de l'article 29 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale.
- CCT n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.
- Normes minimales de la BCSS.
- Normes ISO 27001, ISO 27002 : 2013, ISO 2700.
- Politique de sécurité de l'information de la BCSS[2]
- Recommandations de la Commission de Protection de la Vie Privée[3].

5. RESPONSABILITÉS

La responsabilité de la bonne application de la politique de sécurité au sein du CPAS appartient au responsable de la gestion journalière : le/la Directeur(-trice) général(e) du CPAS.

[2] https://www.ksz-bcss.fgov.be/fr/securite-et-vie-privee/publications/politique-de-securite-de-linformation
[3] https://www.privacycommission.be/fr

Au sein du CPAS, il doit être procédé à la désignation formelle d'un (une) Conseiller(e) en Sécurité qui sera en charge de veiller à la mise en œuvre et au respect de cette politique de sécurité[4].

Ce dernier rapporte au/à la Directeur(-trice) général(e) du CPAS pour toutes les matières de sécurité.

Les personnes en charge de l'infrastructure informatique (matériel, réseau et logiciel) internes ou externes (notamment l'agent du service informatique attitré pour le CPAS) sont tenues de travailler en conformité avec les principes de sécurité, définis par le CPAS, et d'apporter leur soutien au Conseiller en sécurité et aux utilisateurs pour qu'ils puissent respecter cette politique de sécurité dans leur travail.

Conseiller en sécurité dans le CPAS	
Contexte	L'Arrêté royal du 12 août 1993 (M.B. 21.08.1993) relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale, impose à toutes les institutions de sécurité sociale, dont les CPAS, l'obligation d'instituer un service de sécurité de l'information. Le service de sécurité de l'information doit être placé sous la direction du Conseiller en sécurité.
Description de fonction	Le Conseiller en sécurité est chargé de la sécurité des données qui sont traitées ou échangées par son institution. - Il fournit des avis qualifiés à la personne chargée de la gestion journalière et exécute les missions qui lui sont confiées par cette même personne. - Il rédige les règles en matière de sécurité des données, en assure leur évolution, les fait approuver par le Conseil de l'action sociale et les communique au personnel du CPAS. - Il présente auprès du responsable de la gestion journalière un projet de rapport de sécurité annuel et un plan de sécurité trisannuel, avec indication des moyens nécessaires à son exécution. - Il coordonne la rédaction du plan catastrophe propre à son institution de sécurité sociale. - Il veille à l'application des normes minimales de sécurité au sein de son institution. - Il est l'interface privilégiée du service « sécurité » de la Banque Carrefour de la Sécurité Sociale. - Il veille au respect des procédures en matière d'accès des

[4] Pour les modalités de désignation et de description de fonction du Conseiller en sécurité, voir l'encadré ci-dessous.

	utilisateurs au réseau. - Il veille à instaurer et encourager une culture de la sécurité auprès des employés. Les responsabilités du Conseiller en sécurité sont définies dans l'Arrêté royal du 12 août 1993 1993 relatif à l'organisation de la sécurité de l'information dans les organisations de sécurité sociale. Toute intervention planifiée ou non doit d'abord être notifiée au Conseiller au sécurité qui devra marquer son accord de principe avant son exécution.
Désignation	Pour les CPAS, la désignation du Conseiller en sécurité se fait par le Conseil de l'action sociale et doit être communiquée au SPP Intégration Sociale. La personne désignée doit ensuite compléter le « questionnaire d'évaluation pour le candidat conseiller en sécurité » sur le site de la Commission de la protection de la vie privée. La candidature du conseiller sera évaluée par la Section Sécurité Sociale du Comité sectoriel de la Sécurité Sociale. Madame/Monsieur *[XXX]* a été désigné(e) en tant que Conseiller en sécurité lors du Conseil de l'action sociale du *[date].* Cette désignation a été adressée au SPP Intégration Sociale en date du *[XX/XX/XXXX].* Madame/Monsieur *[XXX]* a été désigné(e) en tant qu'adjoint(e) au Conseiller en sécurité lors du Conseil de l'action sociale du *[date].*

6. ASPECTS OPÉRATIONNELS

Le détail opérationnel de cette politique de sécurité est repris dans la deuxième partie de ce document. Cette section est susceptible d'évoluer en fonction des exigences des normes de sécurité ou de l'environnement de travail au sein du CPAS.

7. RESPECT DE LA POLITIQUE DE SÉCURITÉ ET AUDIT

Cette politique de sécurité doit être vérifiée chaque année et mise à jour si nécessaire afin de respecter les exigences légales et contractuelles en matière de sécurité ou pour tenir compte de l'évolution de l'organisation et du contexte de travail du CPAS.

Ce respect des exigences (conformité aux normes minimales de sécurité imposée par la BCSS) sera établi par un audit formel (une fois tous les 4 ans au minimum).

Par ailleurs, toute institution de sécurité sociale est tenue de remplir annuellement, de façon minutieuse, un questionnaire relatif au respect des normes minimales obligatoires en matière de sécurité physique et logique et de transmettre ce questionnaire à la Banque Carrefour de la Sécurité Sociale.

Le Conseiller en sécurité veillera à compléter ce questionnaire dans les délais impartis.

De plus, un rapport annuel et plan de sécurité trisannuel d'actions en matière de sécurité seront établis, mis à jour par le Conseiller en sécurité et soumis à l'approbation formelle du Conseil de l'Action Sociale.

Ce plan de sécurité trisannuel contiendra une liste d'actions à entreprendre, un timing ainsi que les estimations budgétaires requises.

8. PLATEFORME DE SÉCURITÉ

Au sein du CPAS, une plateforme de sécurité est définie, comprenant le/la Présidente du CPAS, le/la Directeur(-trice) général(e) du CPAS, le Conseiller en sécurité et l'Agent du service informatique.

Cette plateforme est habilitée à prendre des décisions et à les faire exécuter suites aux suggestions et recommandations faites par le Conseiller en sécurité.

9. DOCUMENTS ANNEXES

Pour les aspects opérationnels et pratiques, ce document est complété obligatoirement par les documents suivants :

- Charte Informatique en vigueur au CPAS (approuvée par le Conseil de ce [*XX/XX/XXXX]*).
- plan de continuité (appelé aussi plan catastrophe) décrivant la procédure à suivre pour assurer la continuité des services du CPAS en cas d'incident majeur (perte du bâtiment, perte du serveur informatique, interruption des moyens de télécommunications).

Cette politique formelle est approuvée par le Conseil de l'action sociale en date du *[XX/XX/XXXX]*.

EXEMPLE DE POLITIQUE FORMELLE DE SECURITE POUR LES CPAS : ASPECTS OPÉRATIONNELS

1. DOMAINES OPÉRATIONNELS VISÉS PAR CETTE POLITIQUE DE SÉCURITÉ

Les normes minimales « ISMS (Information Security Management System - Normes minimales 2015 » sont d'application.

Il s'agit des normes minimales que les institutions sociales doivent obligatoirement respecter si elles souhaitent accéder (et continuer à avoir accès) au réseau de la Banque Carrefour.

Les normes ont donc une valeur contraignante.

La version à jour est disponible sur le site de la Banque Carrefour via le lien suivant :

https://www.ksz-bcss.fgov.be/binaries/documentation/fr/securite/normes_minimales_securite_2015.pdf

Les aspects opérationnels propres à chacun des domaines, identifiés ci-dessous, sont repris dans une série de procédures ou de règles spécifiques, élaborées et tenues à jour par le Conseiller en sécurité et approuvées par le Conseil lors de la lecture du rapport annuel.

Le point de la sécurité sera inscrit au moins une fois par mois à l'agenda du Conseil de l'action sociale (éventuellement avec la mention '*nihil*' mais de façon à maintenir une vigilance constante de la part de tous les membres du Conseil) ou dès que cela s'avère nécessaire et sera présenté par le/la Directeur(-trice) général(e).

1.1 SÉCURITÉ LIÉE AUX PERSONNE

Le principe du secret professionnel s'impose aux CPAS tant par le Code pénal (article 458) que par les articles 36 et 50 de la Loi organique du 8 juillet 1976 des CPAS.

- Article 36, alinéa 3 : « *Les membres du conseil et du comité de gestion de l'hôpital ainsi que toutes les autres personnes qui, en vertu de la loi, assistent aux réunions du conseil, du bureau permanent, des comités spéciaux et du comité de gestion de l'hôpital, sont tenus au secret* ».

- Article 50 : « *Les dispositions de l'article 36, troisième alinéa, et de l'article 37, alinéas 1er, 2 et 3, sont également applicables aux membres du personnel des centres publics d'action sociale* ».

L'article 28 de la loi organique du 15 janvier 1990 de la Banque Carrefour de la Sécurité Sociale précise que :

« *Celui qui, en raison de ses fonctions, participe à la collecte, au traitement ou à la communication de données sociales à caractère personnel ou a connaissance de telles données est tenu d'en respecter le caractère confidentiel; il est toutefois libéré de cette obligation lorsqu'il est appelé à rendre témoignage en justice, dans le cadre de l'exercice du*

droit d'enquête conféré aux Chambres par [l'article 56 de la Constitution coordonnée - modifié par l'article 97 de la loi du 12 août 2000 (Moniteur belge du 31 août 2000)], dans le cadre de l'instruction d'une affaire par le [comité sectoriel de la sécurité sociale et de la santé - inséré par l'article 49 de la loi du 1er mars 2007 (Moniteur belge du 14 mars 2007)] de la Banque-carrefour ou lorsque la loi le prévoit ou l'oblige à faire connaître ce qu'il sait ».

Au sein du CPAS, cela s'applique donc :

- aux membres du Conseil de l'action sociale ;
- aux personnes amenées à y assister ;
- aux membres du personnel du CPAS.

Chaque nouvel employé devra être informé de ces directives et procédures par le Conseiller en sécurité dès son arrivée, lors de la signature de son contrat de travail.

À cette fin un document « déclaration de confidentialité » est soumis pour signature à tout membre du personnel entrant.

Ce document est archivé chez le Conseiller en sécurité.

Exemple de déclaration de confidentialité pour les membres du personnel du CPAS

Dans le cadre de mon emploi au sein du CPAS de *[XXX]*, je soussigné(e) *[XXX]* reconnais avoir été informé(e) des règles suivantes et m'engage à les respecter.

<u>Confidentialité de l'information</u>

Dans le cadre de mon emploi, certaines informations confidentielles pourraient être portées à ma connaissance. Sachant que la perte ou divulgation de ces informations pourrait perturber ou mettre en péril les activités du CPAS de *[XXX],* je m'engage à ne pas les communiquer, que ce soit pendant la durée de mon contrat ou au-delà.

De même, je m'engage à ne pas utiliser ces informations dans un but autre que celui de remplir mes obligations professionnelles au sein du CPAS de *[XXX].*

À l'issue de mon contrat de travail avec le CPAS de *[XXX]* je lui restituerai tous les supports d'information et n'en conserverai aucune copie ou extrait.

De surcroît, je m'engage à respecter les procédures définies dans la politique de sécurité de l'information afin de protéger ces informations contre tout accès non autorisé ou contre la destruction.

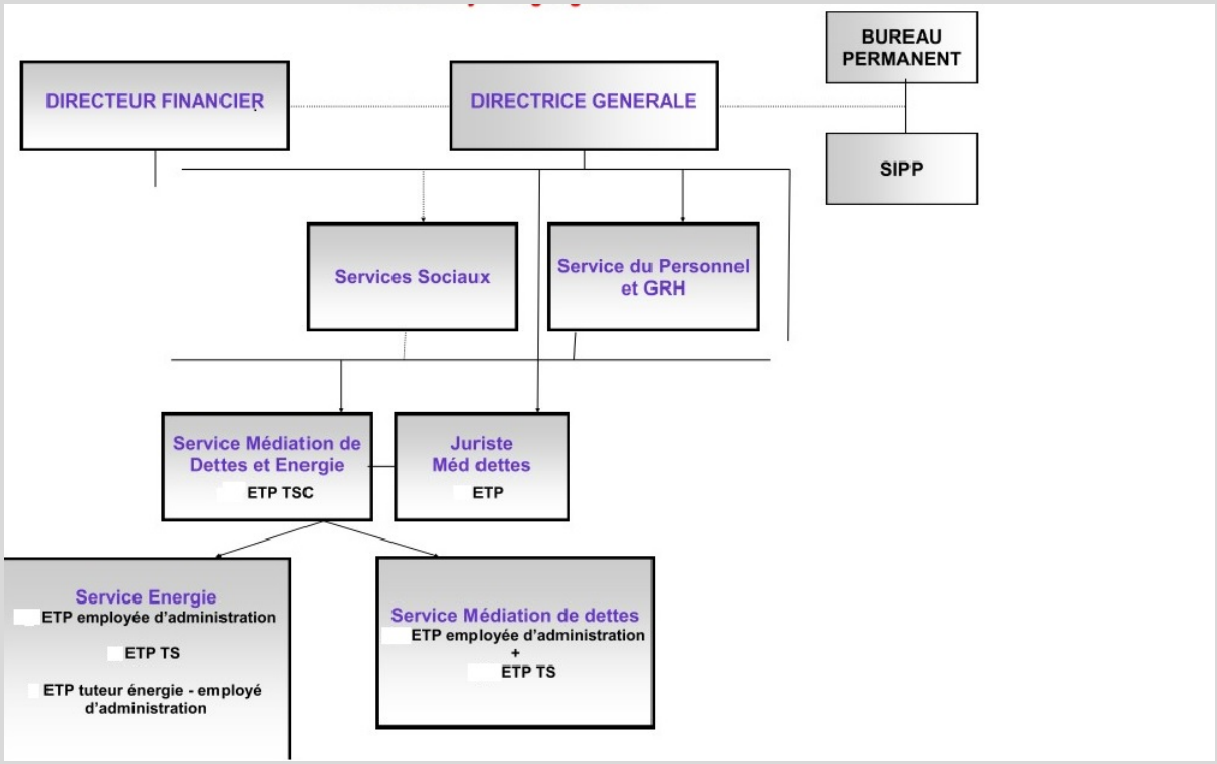
Ces règles sont applicables quel que soit le support de ces informations : papier, audio ou vidéo, informatique, magnétique, optique ou autre.

Sont considérées comme des informations confidentielles, pour autant qu'elles ne soient pas du domaine public ou qu'elles n'aient pas été divulguées par d'autres voies, les données personnelles recueillies par le CPAS dans le cadre de ses missions (Loi organique du 8 juillet 1976 des centres publics d'action sociale) ou relatives à ses agents et toutes autres qui tombent sous l'application la loi du 8 décembre 1992 liée à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

L'employé(e)	**Pour le CPAS de *[XXX]***
Date :	Date :
Nom :	Nom :
Signature :	Signature :

Les personnes faisant partie du CPAS et autorisées à accéder dans le cadre de leur travail aux données à caractère personnel et/ou confidentiel sont reprises dans l'organigramme suivant.

Exemple d'organigramme



1.2 SÉCURITÉ PHYSIQUE

Il s'agit de mettre en place des moyens pour empêcher :

- l'accès non autorisé aux locaux du CPAS, aux locaux des archives du CPAS ou aux informations confidentielles et à caractère social contenues soit dans les dossiers « papier » soit dans les fichiers informatiques ;
- la modification, la perte ou le vol d'informations ;
- l'arrêt de l'outil de travail ;
- tout événement ayant des conséquences dommageables pour le CPAS, tels que :
  - l'incendie et les dégâts des eaux,
  - les intrusions.

Il s'agit également de prévoir les procédures d'évacuation en cas d'incendie ou d'intervention en cas de dégâts des eaux ou d'intrusion.

Par ailleurs, l'accès au local du serveur doit être strictement limité aux personnes reprises dans un inventaire tenu à jour et géré par le Conseiller en sécurité. Seules les personnes identifiées disposeront de la clé (ou du code d'accès) du local.

1.3 PROTECTION DES DONNÉES

Il s'agit d'accorder une importance particulière aux éléments suivants :

a) Accès au réseau

Le CPAS utilise exclusivement un réseau sécurisé et reconnu par la BCSS pour l'accès à internet. Dans le cas présent, le CPAS de *[XXX]*, fait appel au prestataire de services *[XXX]*.

Tout le trafic internet transite exclusivement par cet opérateur (et ses dispositifs de protection - Firewall).

b) Usage d'une déclaration de confidentialité

Lorsque des informations confidentielles pourraient être portées à la connaissance de personnes extérieures/prestataires extérieurs (stagiaires, firmes informatiques…), un document « déclaration de confidentialité » est soumis à ces intervenants et signé par ces derniers.

Exemple de déclaration de confidentialité pour des personnes étrangères au CPAS.

M.- Mme .....

Employé de l'entreprise / stagiaire .....

Chargé(e) de la mission suivante : .....

Dans le cadre de mes activités pour le CPAS de *[XXX]* certaines informations confidentielles pourraient être portées à ma connaissance.

Sont considérées comme des informations confidentielles, pour autant qu'elles ne soient pas du domaine public ou qu'elles n'aient pas été divulguées par d'autres voies, les données personnelles recueillies par le CPAS dans le cadre de ses missions (Loi organique du 8 juillet 1976 des centres publics d'action sociale), ou relatives à ses agents, et toutes autres qui tombent sous l'application la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Sachant que la perte ou la divulgation de ces informations pourrait perturber ou mettre en péril les activités du CPAS de *[XXX]*, je m'engage :

- à ne pas divulguer ni directement ni indirectement les informations confidentielles à des tiers sans l'accord écrit préalable du CPAS de *[XXX]* ;
- à prendre toute mesure pour respecter cet engagement de confidentialité, notamment afin d'éviter qu'un tiers non habilité puisse avoir accès aux informations traitées ;
- à respecter la discrétion la plus stricte sur toutes les informations concernant le CPAS de *[XXX]* que je serais amené à connaître ou que j'aurais pu connaître dans l'exercice de mes fonctions ;
- à ne pas utiliser ces informations dans un but autre que celui de remplir mes obligations au sein du CPAS de *[XXX]* ;
- à restituer tous les supports d'information et à n'en conserver aucune copie ou extrait ;
- à respecter les procédures qui seront portées à ma connaissance dans le cadre de la politique de sécurité de l'information, afin de protéger ces informations contre tout accès non autorisé ou contre la destruction.

Ces règles sont applicables quelle que soit la forme de l'information : papier, audio ou vidéo, informatique, magnétique, optique ou tout autre support.

La présente déclaration est valable pour une durée illimitée à partir de la signature du présent engagement.

Dans le cas où, de façon intentionnelle ou par négligence, je viendrais à ne pas respecter ces engagements et que le CPAS de *[XXX]* subirait en conséquence un préjudice matériel non négligeable, je suis conscient que ma responsabilité pourrait être engagée et que les relations entre le CPAS de *[XXX]* et mon entreprise/ma personne pourraient être rompues. Ces mesures contractuelles pourraient être associées à des poursuites légales à mon égard, dans le respect de la législation applicable.

[À indiquer pour les entreprises : *Au cas où l'entreprise voudrait invoquer cette responsabilité, elle en préviendrait immédiatement l'organisation contractante et l'employé concerné, par courrier recommandé, en motivant sa position et en prouvant la responsabilité. La rupture des relations et des mesures contractuelles ne pourra être envisagée que si les faits sont prouvés et que l'existence d'un préjudice matériel est reconnue*.]

La personne contractante	Pour le CPAS de *[XXX]*
Date :	Date :
Nom :	Nom :
Signature :	Signature :

c) Directives en matière de sauvegarde des données

Il s'agit de conserver, sur un support physiquement éloigné du CPAS, les données informatiques stockées sur le serveur du CPAS.

Le CPAS de *[XXX]* fait des sauvegardes des données.

[Ces procédures dépendant de chaque CPAS, précisez ici les procédures mises en place dans le vôtre pour ces sauvegardes des données informatiques et des données « papier »].

Les documents obsolètes du CPAS sont soit physiquement détruits (déchiqueteuse) soit archivés *[précisez où les documents sont archivés]*.

d) Directive en matière de mise au rebut du matériel informatique

Il s'agit de prendre des dispositions pour que lors de la mise au rebut ou la reprise de matériel obsolète par un tiers, les données présentes sur les disques durs ou les cassettes de sauvegarde (arrivées en fin de vie) soient effacées de manière définitive et irrécupérables[5] .

Cette « destruction de données » se fait en présence du Conseiller en sécurité ou à tout le moins, celui-ci devra s'assurer que les médias (disques durs, cassettes) sont effectivement vidés avant de signer l'ordre de mise au rebut.

Note : la destruction physique de ces médias reste la solution la plus efficace et la moins coûteuse (ne serait-ce qu'en temps) pour un CPAS.

Ces opérations de destruction ou de reprise de matériel obsolète doivent être consignées dans l'inventaire des interventions dans lequel sont consignées :

- toutes les interventions (planifiées ou non), par du personnel interne ou externe ;
- les opérations telle que :

  - vérification de l'UPS (alimentation de secours du serveur),
  - mise au rebut de matériel (PC, cassettes de sauvegarde, disques durs, clés USB de service…),
  - installation de mises à jour des logiciels applicatifs ou autres,
  - remplacement de jeu de cassettes de sauvegarde.

[5] V. par ex. les logiciels http://www.pcdiskeraser.com/ ou http://www.dban.org/about ou autre équivalent.

Exemple d'inventaire des interventions

N° d'ordre	Date de début d'intervention	Intervenant	Motif/nature de l'intervention	Résultat de l'intervention	Date de fin d'intervention
Par exemple	**XX/XX/XX**	**M./Mme**			

e) Directives en matière de fermeture des bureaux et du rangement des dossiers dans les bureaux

Il s'agit d'éviter que des personnes de passage, invitées ou non, puissent accidentellement avoir connaissance de données à caractère personnel et de données confidentielles (personnel d'entretien des bureaux, visiteur occasionnel, etc.).

Ceci implique aussi bien la discrétion « visuelle » qu'« acoustique ».

Le Conseiller en sécurité fait les recommandations d'usage aux employés et rappelle si nécessaire les principes à respecter.

Le tableau ci-dessous énumère les principes de base à appliquer.

Objectif de la procédure

Les dossiers contenant des données à caractère personnel sont confidentiels et accessibles au personnel et à sa hiérarchie uniquement dans le cadre de l'exercice de sa fonction.

Les dossiers doivent toujours être à disposition du personnel et de sa hiérarchie en cas d'absence de l'employé en charge d'un dossier particulier.

Personnes impliquées

Le personnel ainsi que sa hiérarchie qui a besoin des dossiers personnels dans le cadre de sa fonction.

L'archiviste chargé du classement et du rangement dans le local à archives.

Matériel nécessaire

- Armoire à clés à disposition du personnel impliqué.
- Clé pour chaque local où se trouvent des dossiers personnels.

- Armoire(s) avec clé dans chaque local.
- Clé au local à archives.

f) Directive en matière des risques liés à l'utilisation de l'e-mail, à l'accès à internet et à l'usage des applications de bureautique

Ceci concerne notamment les points suivants :

- protection contre les malwares. *[Précisez ce qui est mis en place par le CPAS à ce sujet]* ;
- procédure de l'utilisation du mail (voir exemple de « disclaimer » ci-dessous). Ce texte est inséré automatiquement par le logiciel de messagerie. Il est interdit à tout employé de le modifier ou de le masquer lors de l'envoi de ses e-mails professionnels ;
- procédure de l'utilisation d'internet et règles de bonne pratique en matière de bureautique ;
- politique d'utilisation interne du matériel informatique (PC, disques durs externes, clés USB…).

Ces procédures et directives font partie des documents **Règlement de Travail au CPAS, charte informatique** tenus à jour par le Conseiller en sécurité et communiqués aux membres du personnel du CPAS.

Exemple de « disclaimer » à insérer automatiquement en fin de chaque mail envoyé par le CPAS[6]

Disclaimer : Ce message reste informel, n'engage que son auteur et ne peut être considéré comme une communication officielle du CPAS de *[XXX]*. Toute correspondance, pour être officielle, doit être revêtue à la fois de la signature du président du conseil de l'action sociale ou du membre du conseil de l'action sociale qu'il délègue et de celle du directeur général ou de l'agent qu'il délègue, conformément à l'article 28 par. 2 de la loi organique des centres publics d'action sociale du 8 juillet 1976.

Ce message et toutes ses annexes sont confidentiels et destinés seulement à l'utilisation de l'individu ou de l'entité à qui ils sont adressés. Si vous n'êtes pas destinataire de ce message, veuillez sans délai en informer son auteur et procéder à la suppression de ce message et de toutes ses annexes. La publication, l'impression, la reproduction, la diffusion et/ou la distribution de ce message et de toutes ses annexes auprès de tiers sont formellement interdites.

[Choix] Ce message a fait l'objet d'un traitement antivirus/il est impossible de garantir que ce message et ses annexes soient dénués de virus. Le CPAS de [XXX] ne peut être tenu responsable de la contamination par un virus.

Le CPAS de *[XXX]* ne peut être tenu responsable d'une modification de son message qui résulterait de la transmission par voie électronique.

Version allégée

Disclaimer : Ce message reste informel. Toute correspondance du CPAS de *[XXX]*, pour être officielle, doit être revêtue à la fois de la signature du président du conseil de l'action sociale ou du membre du conseil de l'action sociale qu'il délègue et de celle du directeur général ou de l'agent qu'il délègue.

Ce message et toutes ses annexes sont confidentiels. Si vous n'en êtes pas destinataire, veuillez sans délai en informer son auteur et procéder à sa suppression.

Notre *disclaimer* est disponible dans son entièreté ici *[mettre le lien]*.

g) Contrôles du trafic internet

Ce point est défini dans la charte informatique.

[6] UVCW, 2014, Modèles de disclaimer de mail.
V. www.uvcw.be/no_index/modeles/disclaimer-mail.doc, [consultation le 1.12.2016].

h) Connexions Wifi

L'usage du Wifi est à proscrire sauf contrainte majeure, formellement justifiée (dépannage temporaire, activité ponctuelle…).

Il ne peut être justifié pour le travail normal des employés du CPAS.
Les PC portables du CPAS, utilisés par des employés du CPAS, verront la carte Wifi de la machine désactivée par le gestionnaire du parc informatique.

Si un PC portable doit pouvoir être utilisé à domicile, pour les besoins du service, et que dans un tel cas, une connexion Wifi s'imposait, l'utilisateur sera prié de s'équiper d'un adaptateur Wifi adéquat (clé USB wifi).

À ce jour, les PC portables ne peuvent sortir du CPAS et n'ont pas de connexion Wifi.

i) Inventaire du matériel et des logiciels informatiques

Un tel inventaire doit être disponible et régulièrement mis à jour (tous les 6 mois ou en cas de changement suite à une opération de maintenance) par le Conseiller en Sécurité ou, à sa demande, par M./Mme *[XXX]* du service informatique.

Exemple d'inventaire du matériel informatique

	Marques	Modèles	Ecrans	Quantité	Personnes
Ordinateurs					
Imprimantes					
Switchs					
Logiciels					

1.4 LA SÉCURITÉ D'ACCÈS LOGIQUE

Il s'agit de protéger les accès aux réseaux, aux applications et aux données. Pour ce faire, on dispose :

- d'une procédure pour la création et la gestion des mots de passe. Ces derniers doivent être régulièrement changés ;
- d'un inventaire des habilitations : un inventaire des personnes (internes et externes) ayant accès à telle ou telle application ou au réseau sera tenu à jour ;
- d'une procédure de sécurité à suivre lors de l'embauche ou du départ d'un collaborateur.

Exemple d'inventaire des habilitations (accès aux applications)

Sont consignés dans ce tableau, de façon exhaustive et actualisée :

- les personnes ayant accès au local du serveur du CPAS (ou de la machine hébergeant la virtualisation) ;
- les personnes ayant accès aux équipements de réseau (Router, Firewall, switches) ;
- les personnes ayant un accès logique au serveur du CPAS (physique ou virtualisé) ;
- les personnes autorisées au sein du CPAS à accéder aux applications spécifiées explicitement ;
- les personnes disposant d'un login pour le domaine du CPAS.

Liste des habilitations (comptes autorisés) - version : [XX/XX/XXXX]					
Applications	**Utilisateurs**				
Logiciel social *[nom du logiciel]*					
Logiciel comptable *[nom du logiciel]*					
Logiciel « salaires » *[nom du logiciel]*					
Accès serveur					
BCSS					
Portail Sécurité Sociale – Rapport Unique					
Accès mutations					
E-box					
E-Procurement					
Fichier central de saisie					
Digiflow					
MediPrima					
…					

Exemple de procédure applicable lors du départ ou de l'embauche d'un(e) employé(e) du CPAS

Lors du départ définitif d'un employé du CPAS, il y a lieu de s'assurer que cette personne ne dispose plus des moyens physiques ou logiques d'accéder aux informations confidentielles.

Pour cela il faut procéder aux opérations suivantes :

Sur le serveur

- Supprimer le compte associé à cette personne,

- Décider comment redistribuer les documents utilisés par cette personne vers d'autres employés (à charge du chef de service).

Vis-à-vis de Publilink

- Demander la suppression du compte publilink (accès au Proxy) et supprimer l'adresse @publilink.
- Installer une redirection vers un employé désigné par le Conseiller en sécurité et activer un message de réponse automatique sur le compte de messagerie de la personne qui quitte (de façon à clôturer « en douceur » le compte de messagerie après 1 mois).

Sur le PC

- Nettoyer le répertoire « Mes Documents ».
- Vérifier le contenu des dossiers de Outlook et décider de la suite à donner aux messages envoyés et reçus. Par la suite, il y aura lieu de supprimer le compte et les dossiers y afférant.

Vis-à-vis des firmes informatiques

- Demander la suppression des accès applications utilisées par cette personne. Pour cela on s'aidera de la liste des habilitations.

Divers
- S'assurer que la personne restitue les clés des locaux et armoires dont elle dispose.
- Inversement lors de l'embauche, il y a lieu d'accorder à la personne nouvellement en place les droits d'accès aux applications la concernant.

1.5 LE PERSONNEL ITINÉRANT : USAGE DE PC PORTABLES, DE SUPPORTS AMOVIBLES

L'ordinateur portable et ses périphériques, mis à disposition de l'utilisateur dans le cadre de ses activités professionnelles, sont et restent la propriété du CPAS.

L'utilisation de l'ordinateur portable est strictement limitée à un usage professionnel dans le cadre de la fonction occupée par l'utilisateur et ne pourra être utilisé à des fins privées.

Afin d'assurer la sécurité du matériel qui lui a été confié, l'utilisateur agira en « bon père de famille » et fera en sorte de protéger le matériel et les données.

Les moyens d'authentification (mot de passe) ne peuvent jamais être conservés avec l'ordinateur portable.

L'installation, la configuration, la mise à jour, la maintenance des logiciels sur l'ordinateur portable doivent être réservées au personnel en charge de la maintenance du parc informatique.

À cette fin, le PC Portable sera configuré dès sa mise à disposition du membre du personnel avec :

- un compte « administrateur » local protégé par mot de passe et réservé au personnel de maintenance (et connu du Conseiller en sécurité) ;
- un compte « utilisateur » local pour le membre du personnel protégé par mot de passe (compte en mode « limité »).

L'ordinateur portable ne peut contenir que des logiciels pour lesquels le CPAS dispose de licences appropriées et nécessaires aux activités du CPAS.

Les données **confidentielles, telles que données à caractère personnel** conservées sur le disque dur, ne peuvent être conservées sur l'ordinateur portable et sur ses appareils périphériques que de manière **cryptée** (un logiciel approprié sera installé et configuré sur les PC portables (par exemple : logiciel standard bitlocker de Microsoft).

Une norme relative aux PC portables est par ailleurs émise par la BCSS[7].

Si des données à caractère confidentiel doivent être échangées au moyen de supports amovibles (clés USB, CD/DVDV, Disques durs externes), ces derniers **devront être cryptés** et cela absolument si ces supports sont amenés à quitter l'enceinte du CPAS.

Si le Conseiller en sécurité autorise l'accès à distance, au moyen de PC portables ou fixes, au réseau du CPAS, il devra impérativement être fait usage d'une solution de type « Teleworking protégé » avec usage d'un VPN configuré avec l'aide du prestataire de service Publilink.

1.6 LA CONTINUITÉ DU SERVICE

La continuité des services du CPAS est un objectif majeur de la Politique de sécurité.

Une alimentation de secours est installée pour le serveur permettant au minimum un « shutdown » programmé en cas de panne de courant.

Cette alimentation de secours doit être vérifiée tous les 6 mois selon les procédures définies par le fournisseur et le résultat consigné dans l'inventaire des interventions[8].

Elle est équipée d'un système de notification d'alarme vers le responsable de la maintenance du parc informatique.

De plus, il existe un plan de secours (voir plan catastrophe) permettant au CPAS de reprendre ses activités en un temps déterminé par le Conseil de l'action sociale en cas de désastre majeur (incendie du bâtiment, perte totale du réseau ou /et du serveur).

[7] http://bcss.fgov.be/binaries/documentation/fr/securite/policies/isms_025_laptop_fr.pdf
[8] Voir exemple supra.

1.7 LA CONSERVATION DES DONNÉES À CARACTÈRE PERSONNEL

La Banque Carrefour et les institutions de sécurité sociale sont tenues de prendre toutes les mesures qui permettent de garantir la parfaite conservation et la confidentialité des données sociales à caractère personnel.

A ce titre l'archivage est réalisé dans un local propre au CPAS de telle sorte que seules les personnes autorisées puissent y avoir accès.

Ce local est protégé contre :

- l'incendie,
- les dégâts des eaux,
- l'intrusion.

1.8 LA GESTION DES INCIDENTS

Le Conseiller en sécurité doit être informé de tout incident de sécurité avéré ou soupçonné.

Chaque membre du personnel, de tout niveau, se doit d'être proactif en matière de sécurité. Par mail, ils peuvent rapporter tout incident au Conseiller en sécurité ou à l'agent du service informatique.

Le Conseiller en sécurité jugera l'opportunité de rapporter ou non les incidents au niveau du Conseil et de suggérer des actions en conséquence.

1.9 LA GESTION DES INTERVENTIONS DE MAINTENANCE

Le Conseiller en sécurité doit être tenu informé de toute intervention planifiée ou fortuite sur l'environnement informatique, effectuée par un fournisseur externe ou un employé du CPAS habilité.

Ces interventions seront consignées par mail dans le tableau « inventaire des interventions »[9] et par année.

1.10 RAPPORT ANNUEL/PLAN DE SÉCURITÉ TRISANNUEL EN MATIÈRE DE SÉCURITÉ

Le Conseiller en sécurité rédige et fait approuver formellement par le Conseil d'action sociale, un rapport annuel et un plan de sécurité trisannuel.

Ce plan identifie les actions, les besoins en ressources humaines et/ou budgétaires.

---

[9] Voir exemple supra.

Ce document est soumis chaque année au Conseil en temps opportun pour la prise en compte des aspects budgétaires.

Historique des changements de ce document

- **Version *[date] :* original (proposition de base)**
  - Version *[date actualisée]*