Charte des utilisateurs des systèmes d'information du CPAS

Cette charte a été élaborée par le groupe des « conseillers en sécurité ».

Pour toute question, merci de contacter Madame Sabrina Jacquet du CPAS de Namur.

081/337 224 - Sabrina.JACQUET@cpasnamur.be

Table des matières

Bases légales

Les obligations légales

- Loi du 3 juillet 1978 relative aux contrats de travail ;
- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de DACP ;
- Loi du 15 janvier 1990 organique de la BCSS ;
- Loi du 11 juin 2002 relative à la protection contre la violence et le harcèlement moral et sexuel au travail ;
- Loi du 13 juin 2005 relative aux communications électroniques ;
- Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées ;
- Loi du 8 août 1983 organisant un Registre national des personnes physiques ;
- Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;
- AR 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 ;
- AR du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale + mise à jour au 22 mars 2013.

Les recommandations

- N°8/2012 du 2 mai 2012 de la Commission de la protection de la vie privée relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail ;
- Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

Portée de la charte

La présente charte est applicable à l'ensemble des agents du CPAS, aux agents amenés à exécuter des missions de contrôle dans le cadre de celle-ci et à toute personne ayant accès aux systèmes d'information du CPAS (par exemple : les sous-traitants).

En octroyant l'accès au téléphone, à l'e-mail et à Internet aux agents, le Conseil de l'Action Sociale poursuit les buts suivants :

- ✓ faciliter la communication interne et externe sans pour autant faire l'économie des correspondances officielles qui restent nécessaires lorsque le CPAS est juridiquement engagé
- ✓ mettre à disposition des agents un outil de travail performant à la pointe des nouvelles technologies
- ✓ encourager l'apprentissage et l'utilisation de ces nouvelles technologies, notamment par la formation

La présente charte, qu'il appartient à tout agent de respecter, est adoptée dans le but :

- ✓ d'informer les agents sur l'usage qu'ils peuvent faire des moyens informatiques et téléphoniques mis à leur disposition par le CPAS
- ✓ de garantir l'intégrité des systèmes d'information du CPAS
- ✓ de maintenir un environnement de travail professionnel
- ✓ de protéger les informations qui sont la propriété du CPAS

tout en garantissant l'équilibre des intérêts de chacun.

Elle est applicable à tout matériel ou tout support connecté aux systèmes d'information du CPAS dont photocopieurs, télécopieurs, téléphones portables, PDA, PC portables, slate, supports amovibles, … (liste non exhaustive) qui permet l'envoi, la collecte, le stockage, … de messages, de données et d'images.

Terminologie

La notion « Vie privée » est à entendre comme faculté d'autonomie, de capacité de l'individu à effectuer des choix existentiels. En la matière, il s'agit du droit pour l'individu de « savoir ce qui se sait sur lui », de connaître les données le concernant qui sont détenues, d'en maîtriser les circuits de communication, d'en contrecarrer les utilisations abusives. La vie privée ne se réduit donc pas à une quête de confidentialité, c'est la maîtrise par chacun de son image informationnelle (Cécile de Terwangne, « Vie privée et données à caractère personnel », politeia, chapitre 1).

La notion « Protection de la vie privée » est une émanation du droit au respect de la vie privée. C'est le droit pour chacun de contrôler ses propres données, qu'elles soient privées, publiques ou professionnelles (Cécile de Terwangne, « Vie privée et données à caractère personnel », politeia, chapitre 1).

Le terme « Agent » désigne tout travailleur, quelle que soit la nature de la relation contractuelle ou statutaire qui le lie au CPAS.

Le terme « Conseil de l'Action Sociale » désigne l'organe de décision.

Le terme « Département Informatique » désigne le service informatique du CPAS.

Le terme « Systèmes d'information » désigne tout média permettant l'enregistrement, le stockage, la diffusion d'informations.

Le terme « Conseiller en sécurité de l'information » désigne la personne chargée de la mission de conseiller en sécurité de l'information. Le terme recouvre également celle de conseiller-adjoint en sécurité de l'information.

Le terme « Données personnelles » vise toutes les données qui concernent une personne identifiée ou identifiable.

Le terme « Contrôle des systèmes d'information » désigne l'action de procéder à une vérification des systèmes d'information.

Le terme « Examen » désigne la décision, prise et communiquée préalablement à l'agent, d'effectuer un contrôle de son usage des systèmes d'informations, réalisé dans le cas d'une suspicion d'abus de ces systèmes.

Le terme « E-mail privé » désigne tout e-mail dont l'objet reprend « Privé ».

Le terme « E-mail syndical » désigne tout e-mail dont l'objet reprend « Syndicat ».

Le terme « Téléphonie et Internet mobile » désigne GSM, Smartphone, tablette, slate, PC portable, tout autre appareil facilitant le déplacement et l'accessibilité de l'agent.

Le terme « Carte SIM » (Subscriber Identity Module) désigne la carte d'accès au réseau de téléphonie mobile.

Responsabilités

En général

Tout équipement mis à disposition doit être géré en bon père de famille.
Chaque agent est responsable de l'usage professionnel des moyens informatiques et téléphoniques mis à sa disposition.

Chaque agent reçoit pour l'usage informatique un code d'accès strictement personnel qu'il ne peut communiquer à autrui (sauf exception soumise à l'appréciation du supérieur hiérarchique et autorisation du conseiller en sécurité).

Le téléphone et le matériel informatique (matériel et logiciel) sont des outils de travail qui appartiennent au CPAS et qui sont mis à la disposition des agents.

Tout matériel mis à disposition par le CPAS ne peut être connecté à un réseau non géré par le CPAS.
Excepté pour le personnel, les mandataires et les utilisateurs titulaires d'un équipement mobile mis à leur disposition par le Conseil de l'Action Sociale dans le cadre de leur activité professionnelle, de leur mandat.
Comme il est aussi interdit de connecter tout matériel n'appartenant pas à celui du CPAS et d'exécuter volontairement des programmes ne faisant pas partie de la propriété du CPAS.

En aucun cas, les logiciels installés par le CPAS ne peuvent être copiés et les configurations modifiées.

Chaque membre veille à l'intégrité de ces outils de travail et à ne pas gêner les autres utilisateurs, de même que la bonne conduite des activités du CPAS, par une utilisation excessive des ressources, notamment lors du transfert d'information avec l'extérieur, sur le réseau interne ou sur les espaces de stockage.

Sauf exception, il est interdit d'accéder à des données d'un agent sans son autorisation.

Responsable du traitement

Le responsable du traitement des données de télécommunication en réseau visées par la présente charte est le Conseil de l'Action Sociale.

Gestion des accès par login et mots de passe

Tout agent disposant d'un accès aux systèmes d'information du CPAS reçoit un/des login pour lequel il choisit un/des mots de passe.

Il est interdit de communiquer tout mot de passe, ainsi que de tenter de décrypter ou de découvrir un mot de passe d'un autre agent.

Dans le cadre de leur gestion des systèmes et des applications, le département Informatique peut transmettre des mots de passe temporaires aux utilisateurs. Il s'assure de la transmission confidentielle de ces mots de passe.

Tout agent peut à tout moment changer ou réinitialiser son mot de passe. Le Conseil de l'Action Sociale oblige cependant un changement de mot de passe tous les 30 jours.

Politique du mot de passe

Chaque utilisateur est identifié dans le réseau du CPAS par deux éléments :

- ✓ Son UID (user identification) – c'est- à-dire son nom d'utilisateur
- ✓ Son mot de passe

Le user identification est défini par le gestionnaire du système du département Informatique afin de pouvoir gérer plus facilement les accès des différents utilisateurs.

Quelques règles s'appliquent aux mots de passe afin de les sécuriser :

- le mot de passe est strictement personnel, il ne peut être confié à un tiers
- un mot de passe est unique, il est vivement conseillé de ne pas utiliser deux fois un même code ni de les réutiliser mais bien de les renouveler
- un mot de passe doit être changé régulièrement, pour rappel, la périodicité définie au sein du CPAS est de 30 jours
- l'idéal est de disposer d'un mot de passe difficile à trouver mais facile à retenir (voir l'annexe des conseils pratiques)
- l'agent évitera d'inscrire son mot de passe sur son sous-main ou sur un petit papier collé au PC, ainsi que dans un fichier électronique
- l'agent n'utilisera pas un programme permettant de se rappeler ses mots de passe à tout moment (ces programmes sont souvent des utilitaires pouvant eux-mêmes être utilisés par l'extérieur pour trouver vos mots de passe)
- lorsqu'il quitte, même temporairement, son poste de travail, l'agent activera son écran de veille désactivable uniquement en introduisant son mot de passe
- il veillera à ne pas taper son mot de passe devant une personne susceptible de le lire
- il est interdit par quelque moyen que ce soit de tenter de connaître ou de voler le mot de passe d'une autre personne

- lorsqu'un mot de passe est utilisé fautivement 5 fois de suite, l'accès aux systèmes ou aux programmes est bloqué automatiquement et seul le département Informatique pourra rétablir l'accès

Il est interdit d'exiger d'un agent qu'il communique son ou ses mots de passe pour quelle que soit la raison.
Si la situation se présente, l'agent est invité à prendre contact avec le conseiller en sécurité.

Les agents qui ont accès à une boîte mail générique utilisent leur propre login et mot de passe pour s'y connecter.

Règles pour le mot de passe

Les ressources informatiques du CPAS présentent la caractéristique d'intégrer deux environnements propres (Windows et IBM iseries).
Par conséquent, des règles sont recommandées afin :

- ✓ d'homogénéiser les mots de passe
- ✓ de garantir l'élaboration de mots de passe complexes
- ✓ de faciliter la signature de l'utilisation
- ✓ longueur minimum : 6 caractères
- ✓ longueur maximum : 12 caractères
- ✓ composition : au moins un caractère alphabétique
  au moins un caractère numérique
  au moins un caractère spécial

Confidentialité

L’agent s'engage à ne divulguer aucune information concernant les activités du CPAS, ni aucune donnée relative aux bénéficiaires dont il pourrait avoir connaissance dans l'accomplissement de ses fonctions et qui serait de nature à porter préjudice au CPAS.

Cette obligation de confidentialité s'applique tant à l'égard des tiers que des agents.

Elle gardera tous ses effets pendant toute la durée de la relation de travail et se prolongera après la rupture de celui-ci pour quelque motif que ce soit.

Déontologie

Le Conseil de l'Action Sociale désigne les agents qui sont habilités, en vertu de la présente instruction, à exercer une mission de contrôle, d'examen, de maintenance ou d'assistance. La liste des agents désignés doit être approuvée par le Conseil de l'Action Sociale.

Ces agents ne pourront accéder qu'aux seules données dont ils ont besoin pour l'exercice de cette mission et ne pourront les communiquer que dans le respect des procédures écrites se rapportant à leur mission.

Dans le cadre de l'exercice de cette mission, ils sont tenus à un devoir de confidentialité et s'exposent à des sanctions en cas de violation de celui-ci. C'est le Directeur général qui se réserve le droit de recourir aux sanctions reprises au règlement de travail.

Les administrateurs systèmes et les personnes disposant de privilèges avancés sur les systèmes d'information sont tenus de signer le code de déontologie spécifique à leur mission.

Le conseiller en sécurité de l'information, quant à lui, est tenu de respecter le code d'éthique et bonne conduite le concernant.

Contrôle des systèmes d'information et examen de l'utilisation faite par les agents

Le matériel informatique et téléphonique est propriété du CPAS.

Le Conseil de l'Action Sociale est fortement attaché au principe du respect de la vie privée des agents sur le lieu de travail et respecte par conséquent les principes contenus dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Lorsque l'agent désigné responsable des contrôles effectue un contrôle des systèmes d'information ou un examen de l'utilisation faite par un agent, il s'engage à le réaliser dans le respect des principes de finalité, de proportionnalité et de transparence tels que prévus dans cette loi.

Principe de finalité

Le contrôle des systèmes d'information ne peut se réaliser que pour autant que l'une ou plusieurs des finalités suivantes est ou sont poursuivie(s) :

- ✓ la sécurité et/ou le bon fonctionnement technique des systèmes d'information en réseau du CPAS, ainsi que la protection physique des installations du CPAS
- ✓ la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui
- ✓ le respect de bonne foi des principes et règles d'utilisation des technologies en réseau tels que fixés dans la présente charte
- ✓ la protection de la réputation, des intérêts économiques et financiers du CPAS

Principe de proportionnalité

Le Conseil de l'Action Sociale respecte le principe de proportionnalité dans la poursuite de ses finalités.

Le contrôle des systèmes d'information ne peut entraîner une ingérence dans la vie privée de l'agent ou tout au moins qu'une ingérence réduite au minimum dûment motivée.

Ainsi, ne seront collectées en vue de contrôle des systèmes d'information que les données de communication électroniques en réseau qui sont nécessaires, indispensables au contrôle et qui ont un caractère adéquat, pertinent et non excessif par rapport aux finalités poursuivies.

Principe de transparence

Les modalités de contrôle définies dans la présente charte sont portées à la connaissance de tous les agents conformément aux règles applicables au CPAS pour l'adoption du règlement de travail mais aussi de manière individuelle :

- ✓ tout agent accuse réception d'un exemplaire de la présente charte
- ✓ lors de l'acceptation du lien pour accéder à Internet, l'agent déclare avoir pris connaissance de la charte
- ✓ la charte est disponible sur Intranet dans la rubrique « Sécurité ».

Contrôle des systèmes d'information

Sur base de la recommandation n°8/2012 du 2 mai 2012 de la Commission de la protection de la vie privée relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail.

Ce contrôle est l'action de procéder à une vérification des systèmes d'informations.
Le résultat de celui-ci sera affiché sur Intranet pour informer tous les agents des contrôles et du bon fonctionnement des systèmes d'information. Il sera accessible dans la rubrique « Sécurité ».

S'il est suspecté ou constaté un manquement aux présentes directives ou une anomalie dans l'utilisation des systèmes d'information, l'agent désigné responsable des contrôles en informera le conseiller en sécurité qui, en collaboration avec le département Informatique, évaluera le risque et informera, sans délai, le Directeur général. C'est le Directeur général qui avertira l'ensemble des agents et les informera également qu'un examen des données de communication électroniques en réseau sera effectué lorsqu'une nouvelle anomalie de même nature sera constatée.

Contrôle de l'utilisation des comptes individuels

Sur base d'éléments reçus par le Directeur général (voir schéma pour un contrôle), le ~~CPAS~~ Conseil de l'Action Sociale se réserve le droit de générer une liste des comptes utilisateurs exploités sur son réseau à un moment donné et/ou pour une période déterminée.

Cette liste fait mention des informations suivantes :

- ✓ identification des comptes individuels (comptes clients)
- ✓ date et heure d'ouvertures de sessions de travail
- ✓ date et heure de fermetures de sessions de travail
- ✓ nombre de connexions sur le réseau informatique
- ✓ durée des connexions sur le réseau informatique

Lorsque, à l'occasion d'un contrôle ou au départ d'autres sources d'information, il est constaté une anomalie ou un usage interdit ou abusif d'un compte client, l'agent désigné responsable du contrôle en informe, par écrit, le conseiller en sécurité qui, en collaboration avec le département Informatique, évalue le risque.
En fonction de la situation, l'agent sera identifié soit par l'adresse IP, soit login, soit badge, …

Le justificatif fourni par l'agent sera

- ✓ soit suffisant pour classer dans le répertoire des incidents
- ✓ soit insuffisant et le conseiller en sécurité informera alors le responsable de service de l'agent et le Directeur général

C'est le Directeur général qui se réserve le droit de recourir aux sanctions reprises au règlement de travail.

Par anomalie, on entend l'utilisation simultanée d'un même compte individuel sur plusieurs ordinateurs ou des tentatives d'utilisation d'un compte individuel non propriétaire ou encore des tentatives d'utilisation d'un compte individuel sur un ordinateur non propriétaire.
Sauf exceptions relatives :

- à la bonne organisation des services (ex : bureaux d'entretien) ;
- aux utilisateurs titulaires d'un équipement mobile mis à leur disposition par l'administration dans le cadre de leur activité professionnelle.

Contrôle de l'utilisation Internet

Sur base d'éléments reçus par le Directeur général (voir schéma pour un contrôle), le ~~CPAS~~ Conseil de l'Action Sociale se réserve le droit de générer une liste des sites Internet consultés via son réseau, indiquant la durée et le moment des visites. Cette liste ne fait pas directement mention ni de l'identité de l'agent ni de l'adresse IP.

Lorsque, à l'occasion d'un contrôle ou au départ d'autres sources d'information, il est constaté une anomalie ou un usage interdit ou abusif de l'accès à Internet, l'agent désigné responsable du contrôle en informe le conseiller en sécurité qui, en collaboration avec le département Informatique, évalue le risque.
En fonction de la situation, l'agent sera identifié soit par l'adresse IP, soit login, soit badge, …
Le justificatif fourni par l'agent sera

- ✓ soit suffisant pour classer dans le répertoire des incidents
- ✓ soit insuffisant et le conseiller en sécurité informera alors le responsable de service de l'agent et le Directeur général pour examen de l'utilisation d'Internet

C'est le Directeur général qui se réserve le droit de recourir aux sanctions reprises au règlement de travail.

Par anomalie, on entend des connexions longues et/ou fréquentes sur des sites dont l'accès ne peut être justifié d'un point de vue professionnel ou encore des tentatives de connexion à des sites non autorisés.

Contrôle de l'utilisation de la téléphonie fixe

Gestion des coûts liés à l'usage du téléphone fixe, contrôle et sanctions

Le Directeur financier est compétent pour effectuer un contrôle des dépenses téléphoniques pour chaque service concerné.

Ce contrôle a pour objectif d'assurer la gestion et la maîtrise des dépenses téléphoniques exposées par le CPAS. Il est effectué dans le respect de la vie privée des agents. Il n'a pas pour effet d'établir un lien individuel entre les dépenses liées à un poste de téléphone et à un agent déterminé.

Il est général et ponctuel.

Il s'effectue sur base des factures téléphoniques remises par le fournisseur qui contiennent le détail des communications établies par numéro de téléphone.

Ce contrôle s'effectue par comparaison à une moyenne des dépenses.

Contrôle individuel, ponctuel et justifié peut être effectué uniquement dans les cas et conditions ci-après décrites

Lorsqu'il apparaît qu'une facture est anormalement élevée par rapport à la moyenne établie au sein du service, le Directeur financier en informe le responsable de service concerné.

S'il l'estime justifié, le responsable de service peut demander un contrôle plus approfondi des dépenses par poste téléphonique de l'ensemble du service.

Dans cette hypothèse, il en avertit l'ensemble des agents de son service.

Lorsque ce contrôle laisse apparaître qu'un agent fait usage de son poste téléphonique en violation des présentes instructions, le responsable de service peut adresser une demande motivée au Bureau permanent, pour qu'il soit fait un relevé détaillé des communications émises par le poste téléphonique mis à disposition de cet agent.

Lorsque cette autorisation est accordée, elle est communiquée à l'intéressé. Celle-ci précise les conditions, la finalité et la durée de ce contrôle.

Si ce contrôle entraîne une ingérence dans la vie privée de l'agent, celle-ci doit être réduite au strict minimum.

Ce contrôle ne peut donner lieu à une mise sur écoute ou à une prise de connaissance du contenu de la conversation émise.

Si, lors de ce contrôle, il apparaît que l'agent réalise effectivement un usage du téléphone dans le non-respect des présentes instructions, c'est le Directeur général qui se réservera le droit de recourir aux sanctions reprises au règlement de travail.

Contrôle de l'utilisation de la carte SIM

Gestion des coûts liés à l'usage de la carte SIM, contrôle et sanctions

La mise à disposition de la carte SIM est délivrée par le Conseil de l'Action Sociale pour des agents désignés spécifiquement.

Le contrôle se fait sur le respect des conditions d'utilisation définies lors de la mise à disposition de la carte SIM.

Si la carte SIM est mise à disposition pour un usage exclusivement téléphonique, aucune navigation Internet ne peut être reprise dans la facture.

Si la carte SIM est mise à disposition pour un usage exclusivement Internet, aucune communication téléphonique ne peut être reprise dans la facture.

Si la carte SIM est délivrée pour un usage exclusivement professionnel, aucune communication privée ne peut être reprise dans la facture.

Si la carte SIM est délivrée pour un usage mixte professionnel et privé, l'agent supporte les frais des communications privées.

Contrôle individuel, ponctuel et justifié peut être effectué uniquement dans les cas et conditions ci-après décrites

Pour les agents qui ne sont pas de niveau A, il revient au responsable de service de vérifier la liste des montants facturés mensuellement au CPAS et à l'exacte déclaration de l'utilisation du matériel mis à disposition signée par l'agent concerné.

Lorsqu'il apparaît qu'une facture est anormalement élevée par rapport à la moyenne établie au sein de la liste des cartes SIM mises à disposition, le Directeur financier en informe le responsable de service concerné.

S'il l'estime justifié, le responsable de service peut demander un contrôle plus approfondi des dépenses.

Dans cette hypothèse, il en avertit l'agent.

Lorsque ce contrôle laisse apparaître qu'un agent fait usage de son matériel de téléphonie mobile en violation des présentes instructions, le responsable de service peut adresser une demande motivée au Conseil de l'Action Sociale, pour qu'il soit fait un relevé détaillé des communications émises par la carte SIM mise à disposition de cet agent.

Lorsque cette autorisation est accordée, elle est communiquée à l'intéressé. Celle-ci précise les conditions, la finalité et la durée de ce contrôle.

Si ce contrôle entraîne une ingérence dans la vie privée de l'agent, celle-ci doit être réduite au strict minimum.

Ce contrôle ne peut donner lieu à une mise sur écoute ou à une prise de connaissance du contenu de la conversation émise.

Si, lors de ce contrôle, il apparaît que l'agent réalise effectivement un usage du téléphone dans le non-respect des présentes instructions, c'est le Directeur général qui se réservera le droit de recourir aux sanctions reprises au règlement de travail.

Contrôle du courrier électronique

Les messages électroniques sont stockés sur le serveur du CPAS.

Lorsqu'au départ d'éventuelles sources d'information, il est constaté une anomalie ou un usage interdit du système de courrier électronique, l'agent désigné responsable du contrôle en informe, par écrit, le conseiller en sécurité qui, en collaboration avec le département Informatique, évalue le risque.
En fonction de la situation, l'agent sera identifié.
Le justificatif fourni par l'agent sera

- ✓ soit suffisant pour classer dans le répertoire des incidents
- ✓ soit insuffisant et le conseiller en sécurité informera alors le responsable de service de l'agent et le Directeur général pour examen de l'utilisation de la messagerie électronique

C'est le Directeur général qui se réserve le droit de recourir aux sanctions reprises au règlement de travail.

Par anomalie, on entend des facteurs tels que la fréquence, le nombre de messages, des adresses suspectes, la taille et la présence de fichiers joints.

Examen de l'utilisation des systèmes d'information

Par examen, on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un agent identifié ou identifiable.

A la demande motivée du responsable de service (voir schéma), l'agent désigné responsable des contrôles procédera à un examen de l'utilisation des systèmes d'information faite par l'agent s'il suspecte ou constate :

- ✓ une menace à la sécurité et/ou au bon fonctionnement technique des systèmes d'informations en réseau du CPAS, ainsi qu'à la protection physique des installations du CPAS
- ✓ la commission de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui
- ✓ la violation des intérêts économiques et financiers du CPAS

C'est le Directeur général qui se réserve le droit de recourir aux sanctions reprises au règlement de travail.

Habilitation des personnes pouvant procéder à des contrôles des systèmes d'information (et statistiques) et à des examens

Agent responsable du contrôle de l'utilisation des comptes individuels : ***Responsable informatique***
Agent responsable du contrôle de l'utilisation Internet : ***Responsable informatique***
Agent responsable du contrôle des communications téléphoniques : ***Directeur financier***
Agent responsable du contrôle du courrier électronique : ***Responsable informatique***

Pour rappel, la liste des personnes désignées dans le processus de contrôle et de mise en examen doit être approuvée par le Conseil de l'Action Sociale.

Droits de l'agent

Droit d'accès aux données

Dans le cadre de la présente charte, l'agent a le droit de prendre connaissance de toute information le concernant ayant fait l'objet d'un enregistrement par le CPAS.

L'agent a le droit de recevoir une copie des données enregistrées le concernant dans un délai de 7 jours ouvrables après qu'il en a formulé la demande écrite auprès du Directeur général.

Droit de rectification

L'agent a le droit d'obtenir la rectification de toute donnée enregistrée inexacte le concernant. Dans le mois qui suit l'introduction de la demande écrite, le Conseil de l'Action Sociale communiquera sa position ou, le cas échéant, les rectifications apportées aux données relatives à l'agent.

Droit de suppression

L'agent a le droit d'obtenir la suppression de toute donnée enregistrée le concernant qui, compte tenu des finalités du traitement :

- ✓ est inexacte ou
- ✓ dont l'enregistrement, la communication ou la conservation est légalement interdit ou ne respecte pas les présentes directives ou
- ✓ qui a été conservée au-delà d'une période raisonnable, prenant fin un an après la fin des relations de travail entre les parties

Dans le mois qui suit l'introduction de la demande par écrit, le Conseil de l'Action Sociale communiquera à l'agent la suite qui a été donnée à sa demande.

Utilisation des systèmes d'information

L'utilisation des systèmes d'information doit se faire en bon père de famille.

Les comportements suivants sont interdits :

- ✓ la consultation/diffusion de flux audio/vidéo à partir du réseau Internet (streaming)
- ✓ la diffusion ou le téléchargement de données protégées par le droit d'auteur, en violation des lois protégeant le droit d'auteur
- ✓ la retransmission de messages électroniques en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice au CPAS ou à l'auteur du message originel
- ✓ l'envoi de messages ou la consultation de sites de jeux ou de site Internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de message ou la consultation de sites racistes, révisionnistes, érotiques ou pornographiques, de même que les sites prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, des convictions philosophiques ou politiques d'une personne ou d'un groupe de personnes
- ✓ la diffusion d'informations confidentielles relatives au CPAS, à ses partenaires ou aux agents, sauf dans le cadre strict de la conduite des dossiers du CPAS
- ✓ l'utilisation des systèmes d'information dans le cadre d'une activité professionnelle ou politique étrangère à la relation de travail liant l'agent au CPAS
- ✓ la commande de biens et services destinés à la vie privée (biens de consommation, placements boursiers, etc.)
- ✓ la participation, au départ de l'infrastructure du CPAS, à un « forum de discussion » qui n'est pas professionnel
- ✓ l'envoi et/ou, en cas de réception, l'ouverture de fichiers exécutables (fichier .exe), de même que le téléchargement de tels programmes
- ✓ la participation à des « chaînes de lettres », « pyramides » et procédés analogues
- ✓ plus généralement, l'utilisation des systèmes d'information dans le cadre d'une activité illégale, quelle qu'elle soit

Utilisation de l'internet

Le Conseil de l'Action Sociale tolère l'usage d'Internet, à des fins privées, sans autorisation spécifique de la part du supérieur hiérarchique.

L'accès à Internet à des fins privées doit cependant répondre aux conditions suivantes :

- ✓ il doit être occasionnel
- ✓ il ne peut constituer une infraction à la présente instruction et de façon générale, ne peut contrevenir aux dispositions légales

L'utilisation de l'internet doit se faire dans le respect des dispositions visées dans le chapitre « Utilisation des systèmes d'information » de la présente charte.

Les recommandations pour une bonne utilisation d'Internet sont à appliquer :

- ✓ aucun agent ne peut s'exprimer, au nom du CPAS, pour une prise de position politique, religieuse, syndicale, sexiste, …
- ✓ aucun agent ne peut utiliser Internet à des fins de nuire à autrui : réseaux sociaux, …
- ✓ aucun agent ne peut copier les données appartenant au CPAS chez des tiers

- ✓ tout agent qui prend connaissance de faits, textes, images, … nuisibles pour le CPAS a l'obligation d'en informer le conseiller en sécurité qui, en collaboration avec le département Informatique, évaluera les risques et assurera le suivi (ou l'inverse pour autant que le conseiller en sécurité soit informé pour tenir à jour le relevé des incidents).

Utilisation de la téléphonie fixe

Le Conseil de l'Action Sociale tolère l'usage de la téléphonie, à des fins privées, sans autorisation spécifique de la part du supérieur hiérarchique.

- ✓ l'utilisation du téléphone pour des fins privées doit répondre à une nécessité impérieuse. Par nécessité impérieuse, on vise les actes de gestion personnelle qui concerne la santé ou le patrimoine de l'agent ou des membres de sa famille et qu'il est impossible d'accomplir en dehors des heures de travail
- ✓ il ne peut entraver la bonne conduite des activités du CPAS
- ✓ l'agent est autorisé à recevoir sur son lieu de travail des communications téléphoniques personnelles pour autant que celles-ci n'entravent pas la bonne conduite des activités du CPAS
- ✓ l'usage de numéros 1307 et 1304 afin d'obtenir un numéro de téléphone est toléré. Il y a cependant lieu de privilégier la consultation d'un site Internet approprié (ex : www.infobel.be) ou l'utilisation d'un annuaire téléphonique lorsque cela s'avère possible
- ✓ il convient d'éviter, dans la mesure du possible, la déviation des communications d'un poste fixe vers un GSM lorsque l'agent se trouve dans le bâtiment du CPAS. Dans cette hypothèse, il convient d'informer les agents du service du lieu où il peut être joint
- ✓ toute communication téléphonique vers l'étranger se fait par l'intermédiaire de l'accueil. Seuls certains agents bénéficient de l'autorisation de donner des communications téléphoniques à l'étranger lorsque cela s'avère nécessaire en raison de leur fonction. Ces derniers doivent veiller à activer leur code de blocage en cas d'absence
- ✓ pour toutes les communications téléphoniques entre les services du CPAS, les numéros abrégés doivent être utilisés

Les communications interdites

Lors de l'utilisation du téléphone, toute communication téléphonique commençant par le 0900 et numéros dérivés ou 070 est strictement interdite sauf si l'utilisation est strictement professionnelle et admise par le CPAS (ex : Mycertipost pour le certificat digital ONSS)

En outre, est pénalement réprimée :

- ✓ toute communication téléphonique qui est de nature à porter atteinte directement ou indirectement à la dignité d'autrui, qu'elle se réfère au sexe, à l'orientation sexuelle, à l'état civil, à la naissance, à la naissance, à la fortune, à l'âge, au handicap, à la religion, aux convictions philosophiques, à l'état de santé ou à une caractéristique physique d'une personne ou groupe de personnes

- ✓ toute communication qui rentre dans le champ d'application de l'article 442 bis du Code pénal relatif au harcèlement et/ou de la loi du 11 juin 2002 relative à la protection contre la violence et le harcèlement moral ou sexuel au travail
- ✓ plus largement, toute communication dont l'objet est visé par le Code pénal

Utilisation de la téléphonie mobile et de la carte SIM

L'usage de la carte SIM est de trois types :

- ✓ Soit une carte SIM pour un usage exclusivement GSM : soit « usage mixte professionnel et privé » soit « usage exclusivement professionnel ». Aucune utilisation n'est admise pour la navigation Internet.
- ✓ Soit une carte SIM pour un usage mobile Internet (Smartphone) : soit « usage mixte professionnel et privé » soit « usage exclusivement professionnel ». Le mobile permet une navigation Internet.
- ✓ Soit une carte SIM pour un usage exclusivement Internet (tablette, slate) : il s'agit d'un « usage exclusivement professionnel ».

Le matériel de téléphonie et/ou la carte SIM mis à la disposition de l'agent ne peut être utilisé qu'à l'usage pour lequel il est délivré.
Une carte SIM, mise à disposition pour uniquement des communications téléphoniques, ne peut, à aucun moment, être utilisée dans un mobile Internet.
Il en va de même pour les agents qui utilisent leur carte SIM personnelle via la facturation CPAS. Sauf accord préalable du Conseil de l'Action Sociale et prise en charge totale par l'agent du montant de la facture concernant la navigation Internet.

Utiliser ces appareils engendre une exposition plus élevée à des risques importants :

- ✓ les données de l'agent utilisées pour voler son identité
- ✓ la publication des centres d'intérêt de l'agent peut susciter des publicités ciblées et polluantes

Les communications interdites

Lors de l'utilisation du GSM, toute communication téléphonique commençant par le 0900 et numéros dérivés ou 070 est strictement interdite sauf si l'utilisation est strictement professionnelle et admise par le CPAS (ex : Mycertipost pour le certificat digital ONSS).
Ces numéros ne pouvant être bloqués pour l'utilisation des GSM, la facture téléphonique reprenant les numéros et montants seront automatiquement à payer par l'agent.

En général

Un inventaire des matériels mis à disposition des agents est tenu à jour :

- ✓ Ordinateur portable, slate, tablette : ***Département Informatique***

- ✓ GSM, Smartphone: ***Département Informatique***
- ✓ N° de gsm pour l'agent qui garde son GSM : ***Département Gestion financière***
- ✓ Gestion de la domiciliation bancaire : ***Département Gestion financière***
- ✓ Liste nominative des agents disposant d'un dispositif mobile et/ou carte SIM : ***Département Gestion financière***
- ✓ Gestion des cartes SIM (codes PIN/PUK) : ***Département Gestion financière***

Une liste mise à jour quand cela est nécessaire est mise à disposition du conseiller en sécurité.

Aspect logique

- ✓ l'agent veillera à ce que la solution antimalware est installée correctement
- ✓ l'agent veillera à la mise à jour de cette solution
- ✓ l'agent qui télécharge des applications doit veiller à ne laisser l'application exploiter les données du mobile à son insu
- ✓ l'agent veillera à ne pas laisser le mobile conserver une copie de ses données dans le cloud
- ✓ quand le changement de situation de l'agent l'invite à rendre le matériel, il devra veiller à désinstaller ce qui n'était pas d'origine et à supprimer tout ce qui est éventuellement d'ordre privé. Si l'agent ne parvient pas à nettoyer le mobile, il en informera le département Informatique qui l'assistera dans cette démarche
- ✓ l'agent veillera à ne pas donner l'utilisation du mobile à des personnes extérieures au CPAS comme la famille, les amis
- ✓ l'agent disposant d'un GSM (ou facture pour les appels) devra privilégier les communications avec d'autres GSM

Aspect physique

En cas de vol ou perte, l'agent doit contacter :

- le ***Département Patrimoine*** : déclaration, assurance
- le ***Département Informatique***, cellule technique : aspects sécurité

En cas de détérioration : l'agent doit rapporter l'entièreté du matériel au département Informatique

Le CPAS ne procède pas à la géolocalisation.

Aspect sécurité

L'évolution rapide et diversifiée des versions OS, versions applications rend la sécurité très vulnérable.

L'agent est alors tenu d'accepter les conditions d'utilisation reprises ci-dessous :

- ✓ pour l'agent qui refuse l'obligation de sécuriser le matériel et les accès aux données à distance, le Conseil de l'Action Sociale se réserve le droit de ne pas autoriser l'agent à se connecter aux applications et données du CPAS
- ✓ l'agent qui souhaite se connecter avec son propre mobile sur le réseau du CPAS doit pouvoir le faire en ayant une connaissance claire et précise des conséquences que cela implique (sécurisation du réseau, …)
- ✓ l'agent qui utilise le mobile pour accéder à la messagerie du CPAS, accepte les contrôles et backup comme décrits au point « Contrôle des systèmes d'information »

Utilisation de l'e-mail professionnel

Le Conseil de l'Action Sociale tolère un usage non-professionnel des systèmes d'information dans les limites décrite dans la présente.

L'e-mail privé

Le Conseil de l'Action Sociale tolère l'usage exceptionnel et de brève durée, à des fins privées, du système de messagerie électronique, à condition que cet usage soit occasionnel, n'entrave en rien le bon fonctionnement du CPAS, la productivité et les relations sociales au sein du CPAS, ainsi que les relations extérieures au CPAS, et qu'il ne constitue pas une infraction aux présentes instructions et aux dispositions légales et réglementaires.

Si l'agent fait usage de cette faculté, il est tenu d'indiquer, dans l'objet du message, que celui-ci a un caractère privé. Il doit en outre supprimer, dans le corps du message, toute mention relative au CPAS (telle que signature automatique) et toute autre indication qui pourrait laisser croire que le message est rédigé par l'agent dans le cadre de l'exercice de ses fonctions.

L'agent veillera à ne pas surcharger sa messagerie professionnelle par des éléments qui relèvent de la sphère privée (ex : photographies numériques personnelles, contenus multimédia, …)

Tout mail avec l'objet « Privé » sera :

- ✓ soit supprimé automatiquement des éléments envoyés et de la boîte de réception
- ✓ soit placé dans un répertoire de l'arborescence appelé « Privé ».

L'e-mail syndical

Le Conseil de l'Action Sociale accepte que les organisations syndicales et leurs délégués fassent usage de l'e-mail en vue de la diffusion d'informations entre eux, à leurs affiliés ou au Conseil de l'Action Sociale.

Si les syndicats font usage de cette faculté, ils sont tenus d'indiquer, dans l'objet du message, que celui-ci a un caractère syndical. Ils doivent en outre supprimer, dans le corps du message, toute mention relative au CPAS (telle que signature automatique) et toute autre indication qui pourrait laisser croire que le message est rédigé par l'agent dans le cadre de l'exercice de ses fonctions.

Tout mail avec l'objet « Syndical » sera – pour les syndicats comme pour les affiliés : placé dans un répertoire de l'arborescence appelé « Syndicat ».

L'e-mail professionnel nominatif

L'agent qui utilise l'e-mail avec son adresse nominative veillera à ce que le contenu soit strictement professionnel. Les coordonnées de la signature automatique seront mises à jour et pertinentes (les nom, prénom, fonction et numéros de téléphone, fax, gsm sont complets : ces données étant utilisées par l'extérieur du CPAS).

Les agents qui, en raison de leur fonction, envoient des e-mails en lieu et place d'un autre agent, signent l'e-mail en leur nom propre avec la mention « Pour XX ».

L'e-mail générique

Chaque service reçoit une adresse générique du type info@XXX.be, … cette adresse est liée, au minimum, au compte d'un agent actif du service concerné. Chaque responsable de service veillera à exposer la procédure choisie pour son service.

Il est cependant conseillé de privilégier cette adresse dans les en-têtes de courrier et ainsi assurer un suivi de toute correspondance.

En cas d'absence de l'agent

Absence prévue

L'agent veillera à activer le gestionnaire d'absence, en respectant les recommandations mises en place (voir annexe « Gestionnaire d'absence »).

Absence non prévue

En cas d'absence inopinée de l'agent, une procédure de réponse automatique d'absence sera installée, à la demande écrite du responsable de service, par le département Informatique qui en informera le conseiller en sécurité.

Absence et continuité du service

Sur base d'éléments motivés, le Conseil de l'Action Sociale peut consulter tout courrier électronique d'un de ses agents. En tant qu'employeur, il doit pouvoir gérer les communications de son organisation et assurer la continuité du service. Il faut préciser que cette situation n'entre pas dans le cadre d'un examen suite à une anomalie ou d'un contrôle.

Cette procédure impose au département Informatique de pénétrer dans la messagerie professionnelle de l'agent concerné.

Pour que cette consultation se fasse dans de bonnes conditions et dans le respect de la vie privée, le Conseil de l'Action Sociale gardera toujours à l'esprit les trois principes de base :

- ✓ il doit poursuivre un but déterminé
- ✓ il ne peut pas systématiquement tout contrôler
- ✓ l'agent concerné doit savoir que le CPAS peut accéder aux messageries électroniques et effectuer des contrôles et examen

En règles générales

L'agent qui reçoit des messages dont le contenu est interdit ou interpellant est tenu de l'envoyer au département Informatique pour analyse via l'adresse du service Technique (adresse générique de la cellule technique du département informatique).

Pour tout suivi des messages, l'agent laissera le disclaimer choisi par le CPAS.

L'agent qui reçoit un message qui ne lui est pas destiné est tenu d'en respecter la confidentialité et le supprimer.

Annexe – Conseils pratiques

Voici quelques mots de passe à éviter :

- ✓ Votre numéro de téléphone ;
- ✓ Votre nom ou prénom ;
- ✓ Votre numéro de plaque minéralogique ;
- ✓ Votre numéro de sécurité sociale ;
- ✓ Votre surnom ;
- ✓ Le nom de votre conjoint(e) ;
- ✓ Le nom de votre animal domestique : chien, chat, …

Un bon mot de passe ne figure pas non plus dans :

- ✓ Un dictionnaire ;
- ✓ Une revue ;
- ✓ Un recueil de bons mots ;
- ✓ Un recueil de prénoms ;
- ✓ Un fichier ou listing informatique.

Quel mot de passe choisir ?

- ✓ Par définition, un mot de passe doit avoir :
- ✓ Au moins 8 caractères ;
- ✓ Des chiffres, des lettres et des caractères tels que : -, +, :, etc.

Attention, éviter les lettres avec accent telles que : é, è, ê, ë, …

Quelques astuces

Le titre d'un livre ou d'un film

Exemple : Alice au pays des merveilles

En prenant la première lettre de chaque mot de ce titre peut être extrait le mot de passe suivant : aapdm. Comme ce mot de passe est toutefois trop facile à casser par un pirate et qu'il devra être changé tous les 30 jours, on lui rajoute un chiffre ou une séquence.

Exemple : aapdm0803 (mois et année), aapdm3803 (numéro de la semaine et année).

Pour répondre aux normes de sécurité, on rajoute $. Exemple : aapdm3803$. On peut naturellement compliquer le mot de passe à volonté en prenant la deuxième lettre de chaque mot ou les deux premières lettres de chaque mot.

Le cryptage maison

On peut appliquer une autre technique très simple. En choisissant le titre d'un film ou d'un livre, on prend la première lettre de chaque mot et on intercale le nombre de lettres de chaque mot.

Exemple : Voyage Autour De Ma Chambre (de Xavier de Maistre) donnera le mot de passe suivant : v6a6d2m2c7.

Une autre possibilité est vadmc66227 et rajouter un symbole tel que +, $, =, …

Eviter toutes de former un mot ayant une signification car les logiciels utilisés par les pirates utilisent des dictionnaires.

L'association

L'association des mots peut également être utilisée pour élaborer un mot de passe mais il faudra veiller à le compliquer.

Exemple : *lavitaebella* devra être complété avec des signes : la+vita-e/bella*, mot de passe auquel des chiffres devront être rajoutés.

A noter que la fiabilité de ce mot de passe n'est pas la meilleure.

La simplification

Cette technique consiste à supprimer toutes les lettres en double dans un mot.

Exemple : « serveur » devient servu » auquel on peut rajouter les chiffres suivants : nombre de lettres du mot serveur et nombre de lettres du mot de passe ainsi que l'année et le symbole : servu7503*

Conclusion

A chaque agent de trouver la combinaison qui lui semble la plus facile à retenir sans jamais oublier qu'aucun mot de passe n'est inviolable.

Néanmoins, si les conseils ci-dessus sont appliqués, il sera cependant nécessaire au pirate de passer beaucoup plus de temps pour le craquer.

Annexe – Gestionnaire d'absence

Recommandations pour l'utilisation du gestionnaire d'absence

- ✓ penser que le message pourrait aussi être lu par l'extérieur
- ✓ indiquer le nom complet du collègue de contact
- ✓ indiquer le numéro de téléphone complet, ainsi que l'adresse électronique de contact
- ✓ le message doit être professionnel : éviter « Je suis en congé ; Je suis au soleil ; … »
- ✓ le message doit être mis à jour à chaque absence : les dates !
- ✓ le gestionnaire d'absence doit être désactivé dès le retour de l'agent
- ✓ l'agent qui reçoit le message d'absence erroné d'un autre agent ne manquera pas de lui signaler pour correction

Annexe – Code éthique de bonne conduite du Conseiller en sécurité

I - PRELIMINAIRES

Le code éthique de bonne conduite pour les conseillers en sécurité a été élaboré par le groupe de travail "Sécurité de l'information" du Comité Général de Coordination de la Banque Carrefour.

1. Le conseiller en sécurité exécute ses missions de sécurité dans le cadre :

a) des articles 24 et 25 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale (appelée ci-après loi sur la Banque Carrefour);
b) des dispositions de l'arrêté royal du 12 août 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale (appelé ci-après AR sécurité).

Par ailleurs, lors de l'exécution de sa mission de sécurité, il s'inspire en particulier :

a) des normes minimales de sécurité à respecter par les institutions sociales en vue de leur connexion au réseau de la Banque Carrefour de la Sécurité Sociale;
b) les directives de sécurité au niveau des institutions participant au réseau géré par la Banque Carrefour de la Sécurité Sociale;
c) le manuel "Sécurité de l'information de la sécurité sociale";
d) le document "Synthèse des principales discussions menées au sein du sous-groupe de travail "Données médicales" en matière de protection des données médicales".

2. Tous les conseillers en sécurité s'engagent à respecter ce code éthique de bonne conduite dans tous ses aspects.

3. Ce texte doit être distribué à l'ensemble des institutions de sécurité sociale telles que visées à l'article 2, alinéa premier, 2°, de la loi sur la Banque Carrefour et en particulier à ses conseillers en sécurité. Par ailleurs, il doit être transmis à tout service de sécurité spécialisé agréé.

4. Grâce à ce code éthique de bonne conduite, les institutions disposent d'un outil supplémentaire lors de la sélection des conseillers en sécurité.

L'adaptation du présent document entre dans le cadre des attributions du Comité Général de Coordination de la Banque Carrefour, sur proposition du groupe de travail "Sécurité de l'information".

II - DEFINITIONS

Article 1er - Définition du conseiller en sécurité

Par les termes 'conseiller en sécurité', on entend dans le présent document toute personne physique :

a) dont question aux articles 24 en 25 de la loi sur la Banque Carrefour et dont question à l'article 4 de l'AR sécurité, notamment le conseiller en sécurité et ses adjoints éventuels ;
b) dont question à l'article 11 de l'AR sécurité, notamment les membres d'un service de sécurité spécialisé agréé.

Article 2 - Définition de l'institution

Par le terme 'institution', on entend dans le présent document l'ensemble des institutions de sécurité sociale telles que visées à l'article 2, alinéa premier, 2°, de la loi sur la Banque Carrefour.

III - REGLES ETHIQUES DE BONNE CONDUITE

Article 1er - Objectivité, impartialité et indépendance
Le conseiller en sécurité doit toujours, peu importe s'il exerce une fonction de sécurité dans une ou plusieurs institutions, faire preuve de l'objectivité, de l'impartialité et de l'indépendance utiles lors de la formulation d'avis et de recommandations. Ces avis et recommandations doivent être formulés avec la compétence requise en la matière.

Article 2 - Conscience professionnelle
Le conseiller en sécurité doit faire preuve de la conscience professionnelle requise.

Article 3 - Caractère interdisciplinaire de la fonction
Le conseiller en sécurité doit être ouvert à d'autres disciplines (p.ex. sécurité sociale, problèmes relatifs aux données médicales, informatique, ...) et s'y intéresser. Le conseiller en sécurité doit également faire preuve d'un esprit ouvert et d'une aptitude à dialoguer avec les autres.

Article 4 - Loyauté
Le conseiller en sécurité adopte les principes de sincérité, d'honnêteté et de fidélité vis-à-vis de l'institution où il exerce sa fonction de sécurité.

Article 5 - Demande d'assistance
Lorsqu'un conseiller en sécurité estime ne pas disposer du temps utile ou des connaissances requises concernant un problème ou un thème de sécurité donnés, il peut conseiller de demander l'aide ou l'assistance de personnes plus compétentes ou plus expérimentées.

Article 6 - Confidentialité
Le conseiller en sécurité s'engage à respecter la stricte confidentialité de toutes les informations qui lui sont confiées ou dont il peut prendre connaissance, qu'il peut entendre ou lire dans le cadre de ses missions ou activités professionnelles, et ce tant en ce qui concerne les informations qui ont trait à sa mission que celles relatives à ses collègues.
Le conseiller en sécurité ne peut déroger à cette règle générale de confidentialité des informations que dans les deux cas suivants :

- ✓ dans les cas prévus par le législateur ;
- ✓ après avoir obtenu l'accord du (des) tiers (institution, collègues, ...) qui sera (seront) concerné(s) par la divulgation.

Le conseiller en sécurité veillera également à ce que cette obligation de confidentialité soit respectée par ses collaborateurs et toute personne intervenant, sous sa responsabilité, dans le cadre d'une mission.

Article 7 - Respect des collègues
Le conseiller en sécurité respecte l'opinion de ses confrères et évite de les discréditer. Il n'entreprend aucune action qui pourrait porter atteinte à l'honneur ou au renom de ses confrères.

Article 8 - Mention des problèmes de sécurité au (sous)-groupe de travail "Sécurité de l'information"

Lorsque le conseiller en sécurité estime que le problème de sécurité auquel il est confronté au sein de l'institution où il exerce une fonction de sécurité peut intéresser les autres conseillers, il peut, solliciter l'accord de la personne chargée de la gestion journalière de l'institution avant de faire rapport au (sous-) groupe de travail "Sécurité de l'information" du problème de sécurité constaté et demander s'il ne risque pas, par cette communication, de discréditer son institution.