Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

1 Introduction.

Ce guide a pour but d'aider les conseillers en sécurité des CPAS à :

- comprendre les normes minimales de sécurité créées par le groupe de travail de sécurité de la BCSS - KSZ ;
  aider de manière simple et concrète les conseillers en sécurité à appliquer les normes minimales de sécurité ;
- servir de référence en cas d'hésitation.

Le SPP IS complétera ce guide par des formations générales et ciblées et développera des pages internet de sécurité consacrées aux problèmes posés par les conseillers en sécurité.
Cependant, les conseillers en sécurité du SPP IS qui tiennent des permanences le mardi ne pourront répondre à vos questions que de manière générale car ils ne sont pas au courant de la situation spécifique de chaque CPAS. En effet, ils ne connaissent pas la disposition des lieux, l'environnement informatique ni tous les programmes utilisés par les CPAS.
Ils s'appuyeront sur ce guide pour vous conseiller lors des contacts qu'ils auront avec vous.

2 Description du document.

Il a été tenté d'expliquer chaque norme minimale de sécurité de la manière la plus simple possible. Ces normes minimales de sécurité résultent de l'application des « Directives en matière de sécurité au niveau des institutions participant au réseau géré par la BCSS »[1].
Il est conseillé de lire, aussi attentivement que possible, les Directives en matière de sécurité au niveau des institutions participant au réseau géré par la BCSS.
Ce document ainsi que la plupart des textes, énoncés dans ce manuel, qui régissent la sécurité du réseau de la sécurité sociale sont disponibles sur le site WEB de la BCSS à l'adresse http://ksz-bcss.fgov.be.
Le site web du SPP IS dispose également d'un FAQ (**F**requent **A**sked **Q**uestion – **Q**uestions **F**réquemment **P**osées).
Le SPP IS a été aidé dans cette tâche par

- le service de sécurité de la BCSS (security@bcss.fgov.be).
- les trois fédérations régionales des Unions des Villes et Communes qui nous ont fait bénéficier de leurs connaissances et de leur expérience;
- de la documentation de l'UVCW[2] et de la VVSG[3] ;
- le service de sécurité spécialisé agréé (SSSA) de la SmalS-MvM ;
- la cellule administrative des CPAS ;
- les conseillers en sécurité des VCCV (Veiligheidsconsulenten coördinatievergadering) ;
- le groupe V-ICT-OR
- certains conseillers en sécurité de l'information de CPAS ;

Ces participants disposent de connaissances, d'expérience et de sources d'informations ouvertes à tous les CPAS partenaires du réseau de la BCSS.
Il va de soi que ce manuel sera revu et amélioré en fonction de l'évolution des normes minimales et des améliorations découvertes au fil du temps ainsi que des nouveautés techniques.
A la fin du guide, vous trouverez les coordonnées précises de ces différents partenaires.

[1] http://www.bcss.fgov.be/documentation/fr/s%E9curit%E9/directives.pdf
[2] Union des Villes et Communes de Wallonie, http://www.uvcw.be/
[3] Vereniging van Vlaamse Steden en Gemeenten, http://www.vvsg.be/nl/over_vvsg/missie.shtml;jsessionid=anu505l71oo3k?

3 Qu'est-ce qu'un conseiller en sécurité ?

Le conseiller en sécurité est une personne qui, au sein de l'institution, au sein d'une association de CPAS ou dans un service de sécurité spécialisé agréé conventionné avec le CPAS s'occupe de l'ensemble des mesures de sécurité appliquées aux données à caractère social. Il est donc amené à veiller à la sécurité :

i. des accès aux données à caractère social (logiciel social, logiciel comptable, dossiers avec des documents contenant des données à caractère social, etc.) ;
ii. de leur utilisation ;
iii. du stockage physique et informatique ;
iv. des utilisateurs de ces données ;
v. de la restauration de ces données ;
vi. du respect de la loi sur la protection de la vie privée (http://www.privacy.fgov.be/textes_normatifs/cct_81_FR.pdf).

La définition complète du conseiller en sécurité est contenue dans l'A.R. de 1993 de la BCSS (http://www.bcss.fgov.be/fr/Legislation/19930812.htm).

Il veillera aussi à:

- organiser les mesures à prendre pour répondre aux conditions minimales de sécurité: rédiger le plan de sécurité, coordonner les actions du CPAS, prendre contact avec les services spécialisés (firmes informatiques, services de sécurité, etc.), sensibiliser les utilisateurs de la connexion aux aspects de sécurité, etc.;
- apporter au Conseil de l'Aide sociale un éclairage sur la politique de sécurité qui soit le plus pertinent pour le centre, dans le respect des normes définies par la BCSS;
- servir de relais entre le Conseil de l'Aide sociale, le Secrétaire, les différents services, les travailleurs sociaux ou administratifs utilisateurs de la connexion, la BCSS, le SPP Intégration sociale, les firmes informatiques, etc.;
- contrôler que les règles édictées en matière de sécurité soient respectées.

3.1 Qui peut être conseiller en sécurité?

Bien que le rôle du conseiller en sécurité revête quelques aspects techniques, celui-ci consiste avant tout en des tâches de coordination et de communication. A cette fin, disposer de compétences didactiques pour sensibiliser ses collègues au respect des normes de sécurité est un atout non négligeable.
C'est pourquoi il n'est pas absolument nécessaire de confier cette tâche à un expert technique mais plutôt à une personne qui dispose de qualités relationnelles et d'un minimum d'intérêt pour les aspects techniques et informatiques.

A noter qu'il n'est pas recommandé de désigner le responsable informatique conseiller en sécurité.

Le conseiller en sécurité ne doit pas être titulaire d'un diplôme ou d'une formation professionnelle spécifique. Une formation peut être néanmoins suivie. A l'heure actuelle, le SPP IS organise des séances d'information tandis que la Smals-Mvm dispense une formation plus technique.

Le CPAS peut désigner un ou plusieurs adjoints pour épauler le conseiller en sécurité dans ses missions.

3.2 Comment désigner un conseiller en sécurité ?

La désignation du conseiller en sécurité doit faire l'objet d'une décision du Conseil de l'Aide sociale. Cette décision qui précise l'identité et les coordonnées professionnelles du conseiller en sécurité et, le cas échéant, de ses adjoints, doit être transmise au Service Sécurité de l'information du SPP Intégration sociale:
SPP Intégration sociale G. Kempgens (conseiller en sécurité)
Boulevard Anspach 1 1000 Bruxelles Tél.: 02/508.86.56 Fax:
Le Conseil de l'Aide sociale doit également déterminer le nombre d'heures attribuées au conseiller en sécurité (et à ses adjoints) pour accomplir sa mission. Il n'existe pas de règle pour déterminer le nombre d'heures nécessaires pour le conseiller en sécurité: cela dépend largement de la situation dans laquelle se trouve votre CPAS. Il va de soi que, une fois les mesures de sécurité installées, seul un suivi doit être effectué. Ce suivi nécessite naturellement moins de temps.

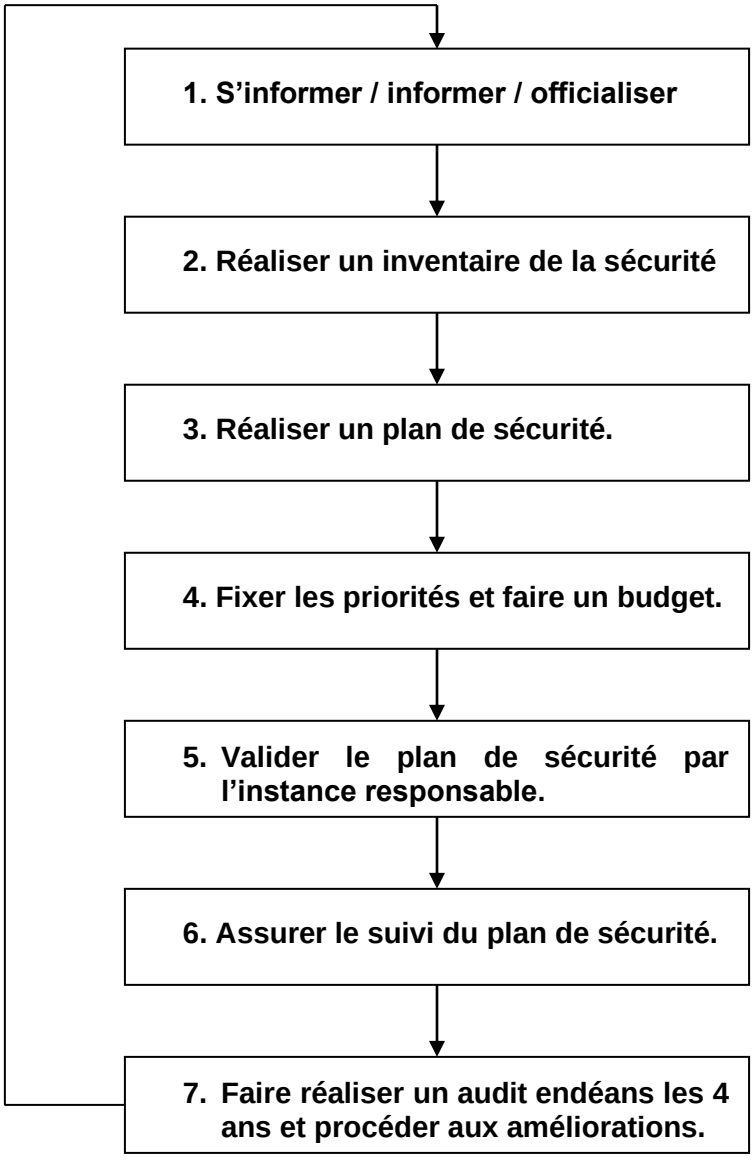
3.3 Que fait un conseiller en sécurité ?

La tâche principale du conseiller en sécurité consiste, à travers le plan de sécurité, à faire en sorte que le CPAS remplisse les conditions minimales de sécurité demandées par la BCSS. Outre les aspects pratiques exposés dans cette partie. La réussite de la politique de sécurité repose également sur le travail de coordination du conseiller: apporter une information pertinente aux membres du Conseil de l'Aide sociale, sensibiliser les utilisateurs au respect des normes, faire le lien avec les fournisseurs du CPAS, etc.
Parmi les normes définies par la BCSS, quatre types de mesures sont développées dans la suite de ce guide:

1. les mesures qui fixent des règles claires en matière de communication et de concertation entre le conseiller en sécurité et les différentes composantes du CPAS;
2. les mesures qui assurent une protection physique des données contre les dégradations matérielles (vol, dégâts lors d'un incendie ou une inondation, panne électrique, etc.);
3. les mesures qui assurent une protection logique des données contre les risques informatiques (virus informatique, perte des données, identification des utilisateurs, etc.);
4. les mesures qui contribuent à la maintenance et aux adaptions des règles de sécurité face aux évolutions techniques (mise à jour des programmes ou du matériel informatique) ou aux événements qui peuvent subvenir.

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

Pour réaliser votre processus de sécurité, nous vous proposons un exemple de plan de travail composé de différentes étapes résumées comme suit :



Lire les directives et les normes minimales. Informer les collaborateurs de votre rôle.

Faire l'inventaire physique (meubles, matériel, locaux, .) et logique (programmes, applications, licences ;).

Faire la liste des tâches à réaliser (voir exemple du plan de sécurité sur le site internet du SPP IS.

4 et 5
Planifier votre travail par trimestre, élaborer un budget pour 3 ans et le faire valider par le conseil de l'aide sociale.

Définir les fréquences d'évaluation et suivre les systèmes de sécurité, les enregistrements, les systèmes de contrôle.

4 Actions à entreprendre en vue de respecter les normes minimales de sécurité.

4.1 Normes minimales de sécurité découlant de l'arrêté royal du 12/08/1993.

Norme 4.1.1 : chaque CPAS connecté au réseau de la Banque Carrefour doit disposer d'un conseiller en sécurité de l'information ou confier la tâche à un service de sécurité spécialisé de l'information agréé.

La personne chargée de la gestion journalière d'un CPAS fixe son choix sur l'une ou l'autre des possibilités proposées en tenant compte :

- des articles 24 et 25 de la loi du 15/01/1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité Sociale ;
- de l'AR du 12/8/1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale ;
- de l'avis N° 99/09 du 9 novembre 1999 du Comité Sectoriel de la Sécurité Sociale relatif à diverses questions posées par le SPF Sécurité Sociale concernant les conseillers en sécurité des CPAS ;
- des besoins spécifiques de son organisation.

1.1 Possibilité n°1 (disposer d'un conseiller en sécurité).
Désigner en interne un conseiller en sécurité : un outil de sélection supplémentaire est mis à votre disposition. Il est intitulé « Code de bonne conduite pour les conseillers en sécurité »[4].

1.2 Possibilité n°2 : (confier la tâche à un service de sécurité spécialisé de l'information agréé).
Il doit s'agir d'un petit CPAS.
Le CPAS adresse la demande préalable au Comité Sectoriel de la Sécurité Sociale et sollicite son approbation.
Afin de permettre au Comité Sectoriel d'apprécier l'importance du CPAS concerné, la demande mentionnera notamment le nombre de membres du personnel, le nombre d'informaticiens, le nombre d'utilisateurs occupés par le CPAS et le nombre de dossiers gérés. le CPAS contacte le service de sécurité spécialisé de l'information agréé afin de fixer les conditions et/ou confirmer la collaboration.

1.3. Possibilité n°3 : désigner un conseiller en sécurité mis à disposition par un ou plusieurs autres CPAS : ceci peut être fait dans le cadre d'une convention (voir possibilité 1.5).

1.4. Possibilité n°4 : créer une association chapitre XII permettant d'engager un conseiller en sécurité.
Une association chapitre XII peut engager un conseiller en sécurité qui se consacrera uniquement à la sécurité au sein de divers CPAS. Cette solution peut être pratique mais il faut également veiller à ne pas confier trop de CPAS au conseiller sous peine de le voir dépassé par la charge de travail.

1.5. Possibilité n°5 : faire appel à une intercommunale ou à un organisme public mettant à votre disposition un conseiller en sécurité moyennant une convention couvrant la mise à disposition.
A noter qu'une personne de la commune peut être désignée comme conseiller en sécurité. Dans ce cas, une convention sera signée entre le CPAS et la commune spécifiant, entre

[4] http://www.bcss.fgov.be/documentation/fr/s%E9curit%E9/bonneconduite.pdf

autres, que le conseiller en sécurité répond uniquement au responsable de la gestion journalière du CPAS pendant ses prestations.
Un CPAS peut également faire désigner un conseiller en sécurité engagé par un organisme public (intercommunale, interrégionale) pourvu que cet organisme ait reçu l'autorisation de la BCSS.

Enfin, il peut encore être bon de préciser que les conseillers en sécurité peuvent se faire conseiller techniquement par un fournisseur privé. Ce fournisseur ne pourra, toutefois, pas être désigné comme conseiller en sécurité.

Plus de détails peuvent être obtenus sur le site web de la BCSS à l'adresse :
http://ksz-bcss.fgov.be/documentation/fr/documentation/s%E9curit%E9/V2002.071.CSICPAS.fr1.pdf

Norme 4.1.2. : chaque CPAS connecté au réseau de la Banque Carrefour doit communiquer l'identité de son conseiller en sécurité et de ses adjoints éventuels au SPP Intégration Sociale.

La personne chargée de la gestion journalière du CPAS communique la décision du conseil de l'aide sociale, par simple courrier au SPP Intégration Sociale, l'identité de son conseiller en sécurité ou du service de sécurité spécialisé agréé de son choix.

La désignation du conseiller en sécurité doit faire l'objet d'une décision du Conseil de l'Aide sociale.

REMARQUES : la connexion du CPAS au réseau géré par la BCSS est conditionnée par la communication, au SPP Intégration Sociale, de l'identité de son conseiller en sécurité de l'information ou de la collaboration avec un service de sécurité de l'information spécialisé agréé.
Afin de favoriser la mission du conseiller au sein d'un CPAS, il est recommandé à la personne chargée de sa gestion journalière d'officialiser cette fonction et d'expliquer aux membres du personnel quels sont les objectifs, les avantages et les obligations du CPAS pour pouvoir utiliser le réseau de la sécurité sociale.

Il n'est pas inutile de rappeler quelques missions de base du conseiller en sécurité qui doit, entre autres :

- présenter au responsable de la gestion journalière du CPAS un projet de plan de sécurité pour une période de trois ans, avec indication des moyens nécessaires à son exécution ;
- coordonner la rédaction du plan catastrophe propre à son CPAS ;
- veiller à l'application des normes minimales de sécurité au sein de son CPAS ;
- être le contact privilégié des services de sécurité du SPP IS et de la BCSS ;
- veiller au respect des procédures en matière d'accès des utilisateurs au réseau.

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

Norme 4.1.3. : lorsque la carte professionnelle pour soins de santé (carte SAM) est utilisée au sein du CPAS, le conseiller en sécurité veille, au sein de son CPAS, à l'utilisation sécurisée de cette carte comme prévu aux articles 42 à 50 de l'arrêté royal du 22 février 1998.

Les cartes SAM sont des puces électroniques semblables à celles qui sont intégrées dans la carte SIS. Ces cartes SAM doivent être utilisées pour pouvoir lire les données inscrites dans la puce de la carte SIS. Certains CPAS les utilisent pour leurs besoins. Dans ce cas, le conseiller en sécurité doit tenir un inventaire :

- des numéros des cartes SAM ;
- des noms des utilisateurs ;
- des numéros des lecteurs de cartes SAM ;

et naturellement tenir ces inventaires à jour. La carte SAM est délivrée par l'INAMI mais M. J. Mertens de la SmalS-MvM (02.509.58.85) peut, à la demande, vous délivrer la procédure existante pour obtenir les cartes SAM et savoir ce que vous devez faire en cas de perte ou de vol.
D'autres informations concernant les cartes SAM et SIS sont disponibles à l'adresse suivante :
http://www.ksz.fgov.be/fr/documentation/document_3.htm.

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

Norme 4.1.4. : chaque CPAS connecté au réseau de la Banque Carrefour de la Sécurité Sociale doit communiquer, à la Banque Carrefour de la Sécurité Sociale, le nombre d'heures officiellement attribuées au conseiller en sécurité de l'information et à ses adjoints éventuels pour l'exécution de leurs tâches.

Le questionnaire annuel est généralement complété par le conseiller en sécurité du CPAS. Il doit, ensuite, être signé par la personne chargée de la gestion journalière du CPAS et transmis au service compétent du SPP Intégration Sociale. Il contient aussi le nombre d'heures consacrées par le conseiller en sécurité à ses tâches.

La détermination du nombre d'heures nécessaires au conseiller en sécurité pour exercer sa mission doit être basée non pas sur une répartition de son temps en fonction d'autre(s) rôle(s) qu'il aurait à jouer au sein du CPAS mais davantage sur des critères tels que notamment le temps nécessaire à :

- exécuter, dans les délais, chaque point du plan de sécurité initial ;
- participer aux réunions internes qui concernent des aspects de sécurité ;
- rédiger et maintenir des politiques de sécurité qui régissent l'accès au réseau géré par la BCSS pour son CPAS ;
- sensibiliser ses collègues à la sécurité ;
- assurer son rôle d'interface pour l'octroi d'autorisation d'accès avec le SPP IS ou la cellule administrative des CPAS;
- participer aux réunions de travail organisées par le SPP IS;
- élaborer les rapports destinés à la personne chargée de la gestion journalière de son CPAS ;
- préparer l'avenir en se formant ou s'informant sur les évolutions technologiques développées au sein du réseau ou utilisées au sein de son organisation ;
- répondre au questionnaire sur les normes minimales ;
- préparer le nouveau plan de sécurité.

Voir le plan de sécurité publié sur le site du SPP IS.

Norme 4.1.5. : chaque CPAS connecté au réseau de la Banque Carrefour doit disposer d'une politique formelle de sécurité de l'information qui est actualisée en permanence.

Une politique de sécurité est un document qui précise l'importance que le CPAS apporte à ses avoirs (mobilier, informatique, savoir, etc.) , les moyens et priorités qui leur sont apportés.

La politique de sécurité de l'information de chaque CPAS doit répondre aux besoins spécifiques de chaque CPAS et être élaborée en conséquence.

Une politique de sécurité est un document créé par le conseiller en sécurité et avalisé par le conseil de l'aide sociale / bureau permanent. Ce document indique quels sont les risques que le CPAS souhaite prendre en considération.

Exemple.

Le CPAS considère que son bon fonctionnement dépend de la connaissance de son personnel en matière d'aide sociale, de revenu d'intégration sociale et de l'ensemble des services qu'il accorde aux gens qui en ont besoin. Le CPAS doit gérer ses ressources avec attention et prendre les mesures appropriées pour les sauvegarder de tout dommage.

Les menaces qui peuvent faire du tort au personnel, aux biens du CPAS et à ses visiteurs comprennent la violence envers les employés, l'accès non autorisé, le vol, la fraude, le vandalisme, les incendies, les catastrophes naturelles, les défaillances techniques et les dommages fortuits. Les menaces de ''cyberattaques[5]'' et les actes malveillants par Internet sont courants et peuvent beaucoup nuire aux services électroniques et aux infrastructures essentielles.

La Politique du CPAS en matière de sécurité prescrit l'application de mesures de sauvegarde pour réduire le risque de préjudice. Elle est conçue pour protéger les employés, préserver la confidentialité, la disponibilité, l'intégrité et la valeur des biens informatiques ou non, et assurer la prestation continue de services. Puisque le CPAS confie des informations à caractère personnel aux technologies de l'information (TI) pour sa prestation de services, cette politique souligne l'importance pour le CPAS de surveiller leurs opérations électroniques.
Le CPAS développera donc une politique à l' égard des risques qu'il considère comme majeurs. Sont pris en considération :

- le personnel ;
- la documentation ;
- les accès aux appareils informatiques ;
- etc.

Il est important de rappeler qu'une politique de sécurité sera plus ou moins stricte en fonction des risques probables : taux de délinquance élevé, proximité d'une rivière, bâtiment ancien en bois, etc.

Le groupe de travail « Sécurité de l'information » du Comité Général de Coordination de la Banque Carrefour de la Sécurité Sociale a élaboré une politique de sécurité intitulée ISMS (**I**nformation **S**ecurity **M**anagement **S**ystem). Ce document de base, commun à l'ensemble des institutions connectées au réseau de la Banque Carrefour, est mis à votre disposition sur le site web de la BCSS. Cependant, il doit être adapté aux besoins spécifiques de chaque CPAS.

Le SPP IS mettra également sur son site internet un exemple de politique de sécurité simplifié à destination des CPAS avant juin 2005.

Le document ci-après est inspiré de l'ISMS réalisé par les conseillers en sécurité de la BCSS.

[5] Une cyberattaque est une attaque menée par une personne bien au courant du fonctionnement des systèmes informatiques et qui souhaite rentrer dans les documents informatiques pour les consulter, les détruire, les modifier, etc.

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

1. Politique de sécurité de l'information Définition des objectifs	Créer une politique de sécurité en y précisant ce qu'on veut protéger en fonction des risques. *Le CPAS est-il près d'une rivière ? Objectif : anticiper les dégâts possibles d'une inondation.* Revoir cette politique en fonction des risques, organiser la sécurité et y mettre les ressources nécessaires.
2. Organisation de la sécurité	Organiser la sécurité en fonction des objectifs. *Par exemple : mettre un détecteur d'eau et s'organiser pour qu'une personne soit prévenue.*
3. Inventaire des ressources analyse des risques.	En fonction de ce que le CPAS souhaite protéger (est défini dans la politique de sécurité), faire un inventaire de ce qui est nécessaire pour diminuer le risque ou pour avoir une solution de rechange. Le risque doit être évalué. *Exemple : quel est le risque d'inondation ? Inondations en 1996 et en 2001, donc risque. Si l'eau monte jusqu'à 50 cm comme en 1996, comment peut-on protéger le serveur ou le PC ? Sinon, comment récupérer les données ?*
4. Sélection et mise en œuvre des contrôles	Choisir une solution proportionnelle au risque. Si les dégâts sont faciles à réparer, ne pas investir inconsidérément. Contrôler ou faire contrôler que le système fonctionne. *Exemple : un détecteur d'eau permettra de réagir à temps et de sauver le matériel. Faire l'entretien du détecteur.*
5. Planning de continuité	La planning de continuité est le document qui doit permettre au CPAS de recommencer à travailler en cas de problème partiel ou total.
6. Formation	Il peut être prévu d'organiser une formation ou de faire suivre une formation pour s'habituer à réagier en cas de problème. *Exemple : exercice d'évacuation des locaux, réinstallation des back-ups, vérifier que la sauvegarde des données a été vraiment effectuée.*
7. Documentation	Documenter les objectifs de sécurité repris dans la politique de sécurité. *Exemple : détail des actions à prendre en cas d'inondation.*
8. Contrôle et audit	Les contrôles sont effectués par le conseiller, l'audit est réalisé par une autre personne. L'audit a pour but de montrer l'efficacité ou non de la sécurité. Il doit permettre de s'améliorer. *Exemple : la procédure à suivre en cas d'inondation a-t-elle tout prévu ? Que fait-on si la personne responsable est absente ?*

Les textes relatifs aux informations énoncées dans ce chapitre sont disponibles sur le site web de la BCSS à l'adresse : http://ksz-bcss.fgov.be/Fr/securite/

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

Les éventuelles améliorations à apporter à la politique de sécurité du CPAS peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

Norme 4.1.6 : chaque CPAS connecté au réseau de la Banque Carrefour doit disposer d'un plan de sécurité approuvé par l'instance responsable du CPAS concerné.

Le plan de sécurité annuel contient des informations décrivant les priorités du conseiller en sécurité au cours des trois prochaines années. Naturellement, si le plan de sécurité rédigé en 2005 prévoit les actions à mener en 2006, il sera fort probablement plus détaillé que pour 2007 et 2008 puisque les priorités seront bien connues et auront évolué avec le temps, l'informatique et la législation.

Le plan de sécurité est la version formelle et écrite de la politique de sécurité du CPAS. C'est l'itinéraire que le conseiller en sécurité doit suivre pour remplir les conditions minimales de sécurité demandées par la BCSS. Il s'agit aussi d'un document justificatif qui rend compte de la politique active du CPAS en matière de sécurité.
Préparé par le conseiller en sécurité, le plan de sécurité doit être approuvé par le Conseil de l'Aide sociale, qui devra être régulièrement (au moins une fois par trimestre) tenu au courant des avancées dans son application et devra approuver les modifications dont le plan serait l'objet.
De plus, le Conseil de l'Aide sociale analysera la possibilité de dégager les moyens nécessaires à l'exécution du plan de sécurité. Si des dépenses sont à prévoir, elles peuvent faire l'objet d'un poste budgétaire spécifique.

Sur base d'un relevé (analyse) des mesures de sécurité existant dans le CPAS, dans les différents domaines de la sécurité de l'information (organisationnelle, sécurité physique, sécurité logique de l'accès aux données, développement et maintenance des applications, protection du réseau, plan de continuité, …) et des mesures encore à prendre pour optimiser la situation et satisfaire ainsi aux normes minimales de sécurité, le conseiller en sécurité de l'information du CPAS pourra établir le plan de sécurité de son CPAS (inventaire des actions à effectuer et des dépenses éventuelles à engager).
Le plan de sécurité, qui peut se présenter sous d'autres intitulés tels que plan d'administration, devra tenir compte de la situation spécifique du CPAS et des moyens de fonctionnement à sécuriser. Dans tous les cas, le conseiller en sécurité devra procéder à l'étalement temporel des actions et des coûts qui en découlent.
Un exemple de plan de sécurité est disponible sur le site internet du SPP IS : http://mi-is.be.

La réussite d'un plan de sécurité est conditionnée par la :

- définition des tâches à accomplir ;
- définition des différents intervenants dans son exécution ;
- définition de la séquence et de la priorité des différentes tâches ;
- mise à disposition des ressources humaines, matériels et financières nécessaires à sa réalisation.

Comme pour l'ensemble des mesures de sécurité, les mesures proposées dans le plan doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Exemple

Norme de sécurité	Situation	Mesures accomplies	Mesures à accomplir	Délais	Budget
Norme 4.3.3. Alimentation électrique alternative	Le CPAS dispose d'un serveur qui centralise toutes les données et les messages envoyés à la BCSS. L'encodage des dossiers transmis à la BCSS se fait directement sur le serveur. Le serveur ne dispose actuellement d'aucune alimentation électrique alternative.	Rien	Achat d'une alimentation de secours à connecter au serveur.	1/1/2006	250 €

Norme 4.1.7. Chaque CPAS connecté au réseau de la Banque Carrefour doit disposer des crédits de fonctionnement nécessaires approuvés par l'instance responsable du CPAS concerné et inscrits dans un budget de sécurité défini séparément, afin de pouvoir prévoir l'exécution de son plan de sécurité.

La mise en place des mesures de sécurité prévues dans le plan de sécurité peut entraîner parfois des dépenses plus ou moins importantes selon leur ampleur. Afin de permettre au conseiller en sécurité d'engager ces dépenses, elles peuvent, avec l'accord de la personne chargée de la gestion journalière, être inscrites dans le budget de fonctionnement du CPAS. Cette organisation permettra au conseiller en sécurité de l'information de disposer du budget nécessaire à la concrétisation des mesures de sécurité reprises dans son plan de sécurité.

Ces crédits sont à associer au plan de sécurité. En fonction des moyens financiers mis à disposition il faudra faire des choix et définir des priorités. La personne chargée de la gestion journalière du CPAS doit à ce niveau pouvoir assurer un rôle d'arbitre et déterminer les priorités parmi les tâches énoncées par le conseiller en sécurité.

Comme pour l'ensemble des mesures de sécurité, l'organisation budgétaire ainsi que les dépenses prévues pour améliorer les mesures de sécurité doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Pour vous offrir une aide concrète, sans toutefois connaître précisément l'organisation comptable de votre CPAS, nous vous proposons d'optimaliser l'inscription du budget « Sécurité » dans le budget global de votre CPAS en concertation avec la personne chargée de la gestion budgétaire et de la personne chargée de la gestion journalière de votre CPAS.
Par exemple : les dépenses envisagées pour réaliser les mesures de sécurité prévues dans le plan de sécurité, pour l'année de références, pourraient soit faire l'objet d'un budget séparé ou d'un/plusieurs article(s) budgétaire(s) distinct(s) avec, par exemple comme titre :

- « Dépenses de fonctionnement pour la sécurité du traitement de l'information » ;
- et/ou
- « Dépenses d'investissement pour la sécurité du traitement de l'information ».

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

4.2 Normes minimales de sécurité définies par le groupe de travail « Sécurité de l'information ».

4.2.1 Organisation de la sécurité.

Norme 4.2.1.1. chaque CPAS connecté au réseau de la Banque Carrefour doit disposer de procédures en vue de la communication d'informations au conseiller en sécurité de sorte que ce dernier possède les données lui permettant d'exécuter la mission de sécurité qui lui est confiée.

Les tâches du conseiller en sécurité comportent une grande part de coordination entre les différentes composantes du CPAS: mandataires, Secrétaire, services sociaux et administratifs, services techniques, etc. La BCSS demande que des mesures formelles de communication et de concertation soient fixées afin que le conseiller en sécurité trouve sa place dans l'organisation du CPAS.

Pour exécuter sa mission, le conseiller en sécurité a besoin d'informations nécessaires sur l'organisation pratique du CPAS. Ce besoin est d'autant plus important si le conseiller en sécurité vient d'intégrer le CPAS ou s'il n'est pas présent au CPAS en permanence: c'est le cas par exemple si le CPAS a opté pour une désignation d'un conseiller en inter-CPAS, la désignation de l'agent communal de prévention ou d'un service de sécurité agréé.
Il faut donc prévoir des procédures formelles qui permettent de tenir le conseiller au courant des éléments qui touchent de près ou de loin les questions de sécurité. Par exemple:

- problèmes de sécurité: quand, où et comment des problèmes de sécurité ont lieu (dégradation du matériel, impossibilité de *se* connecter à la BCSS, attaque d'un virus informatique, etc.);
- organisation des services du CPAS: comment les services sont organisés, qui fait quoi, quel agent est chargé de l'encodage des décisions, quel travailleur social a besoin de consulter des données du réseau de la sécurité sociale, quels sont les changements de personnel (recrutement, départ, changement d'affectation, etc.).

Concrètement et pour l'exemple citons la mise à disposition de procédures orales ou écrites afin d'assurer la participation du conseiller en sécurité aux réunions des différents services (travaux informatiques, prévention et la protection du travail, ….) et /ou la réception des rapports des réunions nécessaires à l'exécution de sa mission.

Norme 4.2.1.2. chaque CPAS connecté au réseau de la Banque Carrefour doit disposer de procédures ayant pour objectif d'organiser la concertation avec les différentes parties impliquées afin d'associer plus étroitement les conseillers en sécurité aux travaux du CPAS.

Les personnes visées par ces procédures sont principalement les membres du service informatique, le conseiller en prévention et en protection du travail, le conseiller en sécurité de l'information ainsi que le service qui gère les données.
Dans ce contexte la personne chargée de la gestion journalière joue un rôle déterminant dans la mesure où elle doit favoriser la participation et l'intégration de son conseiller en sécurité aux différentes structures de l'organisation du CPAS.
Au cas où le conseiller en sécurité ne fait pas partie intégrante du CPAS où s'il n'est présent que périodiquement, il est important que la personne chargée de la gestion journalière veille à tenir au courant les différentes personnes concernées et son conseiller.

Concrètement et pour l'exemple citons la mise à disposition de procédures orales ou écrites afin d'assurer la concertation avec les différents services impliqués afin d'associer plus étroitement le conseiller en sécurité aux travaux du CPAS (concertation avec le service chargé des travaux informatiques, de la gestion des données, de la prévention et la protection du travail, ….). Lorsque le conseiller en sécurité n'est présent que périodiquement, c'est principalement la personne chargée de la gestion journalière du CPAS qui veille à organiser un canal de communication.

Exemple: un conseiller en sécurité a été désigné dans le cadre d'une association de cinq CPAS. Il a été convenu qu'il passe une matinée par mois dans chaque CPAS. Chaque utilisateur de la connexion possède un emploi du temps du conseiller et les coordonnées pour le joindre. Dès lors, si un utilisateur oublie son mot de passe, il contacte le conseiller en sécurité qui éventuellement sur base du contrat passé avec le fournisseur informatique du CPAS concerné, demande soit à l'informaticien du CPAS soit au technicien de la société informatique de fournir confidentiellement un nouvel accès au travailleur. L'utilisateur est tenu d'envoyer une demande écrite ou électronique message électronique au conseiller afin de garder une trace de l'intervention.

Il est également intéressant pour le conseiller en sécurité de tenir un registre des incidents survenus tout au long de l'année. Ce registre peut être tenu sur un carnet ou sur PC et contiendra idéalement les informations suivantes :

Date de l'incident	Nom de la personne ayant constaté l'incident	Origine, nature de l'incident et conséquences	Réponse apportée et action préventive à mener	Date de résolution	Nom de la personne ayant résolu l'incident
12/10/2005	Mme J. Dethiers	Virus dans un fichier. Réseau et PC bloqués pendant 2h.	Scannage du serveur avec un CD de secours mis à jour, suppression du virus et redémarrage du serveur.	13/10/2005	M. J. Secure, informaticien.

Tableau 1

Ce genre de registre est très utile car il permet :

- de garder une trace des problèmes vécus pendant la période de référence (1 an) ;
- de choisir les actions à mener pour corriger les problèmes ;
- d'évaluer éventuellement les pertes financières et en temps occasionnées par les incidents et donc de mieux juger l'intérêt d'investir pour éviter la répétition du ou des problèmes ;
- d'intervenir plus rapidement et anticipativement pour éviter les incidents.

4.2.2 Sécurisation physique et sécurisation de l'environnement.

Norme 4.2.2.1. chaque CPAS connecté au réseau de la Banque Carrefour doit limiter aux personnes autorisées et contrôler, aussi bien pendant qu'en dehors des heures de service, les accès aux bâtiments et aux locaux.

Le conseiller en sécurité de l'information veille à ce que les accès au bâtiment et aux locaux du CPAS soient limités aux personnes autorisées.
Pour émettre un avis compétent en la matière, il devra impérativement inventorier les accès (tant au bâtiment qu'aux locaux) et les différentes catégories de personnes (p.ex : personnel, visiteurs, techniciens) qui auront accès dans quels lieux, sous quelles conditions, à quel moment et sous quelle surveillance. (p.ex : limiter l'accès au local contenant le(s) serveur(s) aux personnes du service, recevoir les visiteurs dans un local dédicacé, derrière un comptoir d'accueil, fermer les locaux sensibles en dehors des heures de prestations, …).

Comme pour l'ensemble des mesures de sécurité, la limitation et le contrôle des accès aux bâtiments et aux locaux, pendant et en dehors des heures de service doivent répondre aux besoins spécifiques de chaque CPAS et être élaborés en conséquence.

Cette limitation d'accès doit être organisée suivant l'importance du CPAS et la disposition de ses locaux, par exemple: contrôle automatique (badge et lecteur), contrôle physique (préposé à l'accueil).
Le contrôle d'accès peut également être situé en un autre lieu, jugé stratégiquement mieux approprié (p. ex : implanté au niveau de l'accès au bâtiment ou aux locaux du CPAS). Dans les petits CPAS, il pourra s'agir simplement d'un espace d'attente réservé aux visiteurs.

Dans tous les cas, il s'agira de tenter d'empêcher que des personnes mal intentionnées puissent facilement accéder :
- au matériel informatique afin de le détériorer/enlever et/ou consulter/modifier/détruire des données confidentielles (p. ex : données sociales à caractère personnel) ;
- aux dossiers contenant des données à caractère social ;
- aux locaux contenant des archives de données confidentielles.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Pistes d'action.

Placer le serveur dans un local auquel le public n'a pas accès et où le passage est limité; ce local devra être fermé à clef.

Exemple:

- *le bureau du Secrétaire, une pièce sans fenêtre, un bureau du service administratif, etc. A contrario, il vaut mieux éviter: la réception, le bureau où ont lieu les permanences, la salle du Conseil, etc. Si toutefois le bureau du secrétaire est trop petit et qu'il n'est pas possible de mettre le serveur ailleurs pour des raisons techniques, le serveur peut être rangé dans une armoire métallique solidement fixée au mur et dotée d'aérations indispensables au refroidissement de l'appareil. Ce genre d'armoire peut être facilement fait à moindre prix par un ouvrier communal.*

Contrôle d'accès dans l'ensemble du bâtiment à l'aide de dispositifs d'enregistrement.

Exemple:

- *certains CPAS, pour éviter au mieux une circulation non désirée dans le CPAS, ont installé à l'entrée du bâtiment un système d'accueil (par exemple une salle d'attente). D'autres ont ajouté un système d'alarme afin de contrôler l'accès au bâtiment en dehors des heures de service ;*
- *certains CPAS utilisent des systèmes à badge donnant accès à certains locaux réservés aux personnes désignées. A noter qu'il est possible d'installer un seul lecteur de badge pour un seul local mais enregistrant les entrées pour chaque personne. Ceci a le mérite de limiter l'investissement ;*
- *sécuriser l'utilisation des clefs et des passe-partout des locaux dits "sensibles". Un système de pavé numérique permet également de limiter les accès aux personnes désignées. Le coût de ce genre de système est inférieur à 1OO € hors installation (système facile à installer).*

Norme 4.2.2.2. chaque CPAS connecté au réseau de la Banque Carrefour doit prendre des mesures pour la prévention, la protection, la détection, l'extinction et l'intervention concernant l'incendie, l'intrusion et les dégâts des eaux.

Les mesures de sécurité contre l'incendie relèvent d'une tâche dévolue au conseiller en prévention et en protection du travail. La protection plus spécifique du matériel informatique dépendra généralement de sa (grande) valeur. Dans tous les cas, ces mesures (prévention, détection, extinction) peuvent être proposées en collaboration avec le conseiller en prévention et les firmes spécialisées agréés. Par exemple, il peut s'agir de l'installation d'une détection incendie (détecteur, centrale d'alarme) et d'une extinction manuelle (extincteurs portatifs) ou d'une extinction automatique.

En ce qui concerne les mesures pour se prémunir contre une éventuelle intrusion, il pourrait s'agir de la fermeture à clef des locaux/bâtiments en dehors des heures de prestations et/ou de l'installation de détecteurs et d'une centrale d'alarme et/ou de l'organisation d'une surveillance physique par une société de gardiennage ou autre.
Améliorer la sécurité à l'aide de petits trucs simples : stores dissimulant les PC et les écrans plats, pastilles indiquant que les locaux sont protégés par un système antivol, installation d'une caméra web, installation d'une fausse caméra (attention, le personnel et les visiteurs doivent être avertis de la présence de caméras).

En ce qui concerne les mesures de sécurité en vue de se prémunir contre les dégâts des eaux et avant de proposer des mesures, il s'agira d'identifier les menaces et de les étudier. Ainsi, on privilégiera surtout, par exemple, l'installation du matériel informatique à l'étage plutôt qu'en sous sol, à l'écart des écoulements possible d'eau, …..). A noter que les locaux informatiques équipés d'un système d'air conditionné ont automatiquement des conduites d'évacuation d'eau. Veillez à ne pas faire passer ces tuyaux au-dessus du serveur ou des gros ordinateurs (mainframe).

De manière générale, un certain nombre d'acteurs sont souvent prêts à vous aider et à vous conseiller souvent gratuitement : pompiers, sourciers de la commune, police, intercommunales de gaz et d'électricité, agent de prévention de la commune, etc…

Pistes d'action.

Eviter de placer les serveurs et PC sous les canalisations d'eaux, au sol, à côté d'une machine à café, à côté d'une fenêtre ou d'un accès au bâtiment. D'autre part, il est important que le serveur ne soit pas soumis à des températures extrêmes; veillez donc à le protéger grâce à un système de ventilation ou de climatisation ou en le plaçant dans une pièce isolée. Pour contrôler les températures auxquels sont soumis les appareils, installer un thermomètre équipé d'un système enregistrant les maximums et les minimums (thermomètre commun et peu onéreux). En principe, le local informatique ne doit pas dépasser les 23° (recommandation HP).

Attention aux CPAS proches d'un cours d'eau et aux risques d'inondation. Veillez toujours à ne pas déposer vos serveurs au sol et à les surélever d'au moins une vingtaine de centimètres. Cette précaution vaut également pour les archives et les fils et câbles électriques.

Attention aux CPAS dont l'installation électrique est vétuste. Souvent, les appareils informatiques sont connectés à la même prise domino. Les risques d'échauffement sont réels et les risques d'incendie en sont accrus.
Dans le même ordre d'idées, placer à proximité de votre serveur un extincteur, de préférence en dehors du local informatique, à l'entrée par exemple. Votre extincteur doit pouvoir éteindre non seulement le serveur mais également les documents (réduits au strict minimum) rangés à proximité pour aider l'informaticien. Ne ranger pas de matériel inflammable à proximité.

Il est préférable de ne pas installer de système d'extinction à eau automatique. Seuls certains gros ordinateurs sont conçus pour résister à des brumisations d'eau.

Envisager de pouvoir remplacer votre matériel informatique en cas de catastrophe et si votre matériel est important. Certains firmes informatiques ou même votre fournisseur de logiciel social peuvent, par contrat, s'engager à vous remplacer votre matériel et à réinstaller vos sauvegardes informatiques dans un délai que vous définirez avec eux.

Eviter également :

- *d'installer votre matériel informatique dans un local situé au sud ;*
- *d'installer un système d'air conditionné si la température de votre local ne dépasse jamais les 23° ;*
- *les prises électriques dans le sol (risques de court-circuit) ;*
- *les faux plafonds communiquant avec d'autres pièces non protégées.*

Préférer :

- *un contrat de dépannage dans les 24h pour votre système d'air conditionné (qui tombera plus facilement en panne quand il est fort sollicité et quand beaucoup d'autres demandes d'interventions arriveront chez le fournisseur) ;*
- *l'installation de vos prises électriques à une dizaine de centimètres du sol au moins.*

Norme 4.3.3. le CPAS doit disposer d'une alimentation électrique alternative permettant de clôturer sans risque les opérations informatiques (lorsque les institutions possèdent un réseau secondaire et/ou lorsqu'elles fournissent des données dans le cadre de la sécurité sociale).

Les appareils informatiques sont assez sensibles aux perturbations dans l'alimentation électrique (coupure, pic ou déséquilibre de tension, …).
Le risque que le CPAS court en absence d'alimentation alternative réside dans la perte du travail effectué à ce moment-là: le travailleur devrait recommencer l'encodage sans forcément savoir quelles données ont été transmises ou non. La durée d'alimentation électrique autonome, nécessaire en cas de panne électrique pour terminer un échange de données, est estimée autour d'une demi-heure.
Sans nécessairement engager des ressources financières importantes, il est possible aujourd'hui d'investir dans des solutions qui permettent d'assurer l'obligation énoncée par cette norme.
Le conseiller en manque d'information sur le sujet peut prendre contact avec son administration de tutelle ou à défaut avec l'un des partenaires recensés à la fin de ce manuel.

Il est recommandé de séparer les câbles informatiques des câbles électriques. Quant aux alimentations auxiliaires et de secours (groupe électrogène par exemple), elles ont pour but d'assurer une alimentation ininterrompue et d'améliorer la qualité de la source d'alimentation. Elles sont malheureusement fort onéreuses. Afin de vous aider dans le choix de l'appareillage, nous vous conseillons de vous adresser au représentant de votre fournisseur de matériel informatique. A titre d'exemple, nous vous signalons qu'il existe une multitude de matériel sur le marché capable d'assurer la sécurité de l'alimentation d'un/plusieurs PC/serveur ou l'ensemble de votre système informatique.
Citons notamment les redresseurs avec batterie d'accumulateurs et alternateur (il y a des UPS[6] disponibles déjà à partir de 250 €) avec ou sans groupe de secours (moteur).

Comme pour l'ensemble des mesures de sécurité, l'ensemble du matériel nécessaire afin de disposer d'une alimentation électrique alternative permettant de clôturer sans risque les opérations informatiques doit répondre aux besoins spécifiques de chaque CPAS.

Attention : pour qu'un UPS parvienne à fournir de l'électricité au serveur afin qu'il clôture ses activités sans perdre les données encodées, ne brancher que le strict nécessaire. Dans le cas contraire, votre UPS qui n'est équipé que d'une batterie ne pourra fournir assez de courant et vos données seront perdues.

[6] Un UPS est une alimentation de secours. Elle peut être une batterie ou un groupe électrogène.

4.2.3 Sécurisation logique de l'accès.

Norme 4.2.3.1. chaque CPAS connecté au réseau de la Banque Carrefour doit sécuriser l'accès aux données nécessaires à l'application et à l'exécution de la sécurité sociale par un système d'identification, d'authentification et d'autorisation.

Quelques définitions préalables s'imposent.
Identification.
Donnée introduite par l'utilisateur afin de permettre, au système informatique, de l'identifier (p. ex : nom et/ou prénom, N° de pointage, Userid, …).

Authentification.
Donnée (mot de passe) introduite par l'utilisateur afin de permettre au système informatique de s'assurer que l'utilisateur est bien la personne qu'il prétend être (code secret, carte à puce, données biométriques, token électronique…).
Veiller à changer régulièrement de mot de passe et à ce qu'il ne soit connu que de l'utilisateur.

Attention à ne pas faire circuler les mots de passe ou à ne pas coller sur l'écran un aide-mémoire avec celui-ci. Vous pouvez vous aider du document disponible sur le SPP IS pour vous aider à choisir des mots de passe faciles à retenir : http://mi-is.be/FR/content/bonnepolitiquedemotdepasse.pdf.

Autorisation.
Limiter l'accès des utilisateurs aux données, service, applications, … nécessaires à l'exécution de leurs tâches.

Le conseiller en sécurité de l'information veillera à ce qu'un tel système de sécurisation d'accès soit fonctionnel avec ou sans l'aide du gestionnaire informatique.

Il est probable que dans le futur l'utilisation d'un TOKEN[7] fonctionnaire ou de la carte d'identité électronique fasse l'objet d'une généralisation dans le processus d'accès au portail de la sécurité sociale (c'est déjà le cas pour le portail fédéral).
Dans ce contexte une POLICE déterminant des règles strictes est disponible sur le site web de la BCSS à l'adresse : http://ksz-bcss.fgov.be/documentation/fr/News/token_fonctionnaire.pdf

Comme pour l'ensemble des mesures de sécurité, les mesures pour sécuriser l'accès aux données nécessaires à l'application et à l'exécution de la sécurité sociale par un système d'identification, d'authentification et d'autorisation *doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.*

[7] Un document explicatif sur le token sera rédigé et remis aux Unions des Villes et Communes et publié sur le site du SPP IS.

Norme 4.2.3.2. chaque CPAS connecté au réseau de la Banque Carrefour doit implémenter un système de logging pour les données à caractère personnel nécessaires à l'application et à l'exécution de la sécurité sociale.

Règles générales.

Définition du ''Logging'': données historiques (qui a fait quoi et quand) permettant, a postériori, d'identifier l'utilisateur, les données / application traitées ainsi que les date/heure de l'opération.

Exemple: le conseiller en sécurité doit être capable de retrouver quel assistant social a consulté les données du registre national via une connexion électronique avec la BCSS le vendredi 11 juin à 11h43 ou quel agent administratif a encodé un dossier le jeudi 10 juin dans le logiciel social.

Le log ou logging est donc un enregistrement, une trace d'une opération réalisée. Selon le niveau demandé, il est possible de retrouver toutes les opérations effectuées.
Seul votre fournisseur de logiciel social sera à même d'installer ce système sur votre programme social (plusieurs fournisseurs de logiciels sociaux disposent de ce système parfois déjà installé). En ce qui concerne votre environnement informatique (Windows 98, 2000, XP, Linux, AS400, etc.) et si cela s'avère nécessaire, des produits sont disponibles sur le marché ou en open source (code informatique public).

Le conseiller en sécurité devra également envisager plusieurs problèmes liés aux loggings avec le responsable de sa gestion journalière et avec l'informaticien si le CPAS en a un :

- que va-t-on enregistrer dans les loggings ? Uniquement les noms des utilisateurs ou leur identifiant, les dates et heures, les programmes et applications concernés ainsi que la nature de la modification ou bien va-t-on également enregistrer la modification elle-même ainsi que d'autres informations ? Dans ce cas, cela implique beaucoup de mémoires pour tout sauvegarder ;
- combien de temps va-t-on sauvegarder les loggings ? La durée de la sauvegarde sera-t-elle décidée en fonction de la date limite de la découverte d'une faute intentionnelle (6 mois) ou plus longtemps selon la nature de l'infraction ?
- sur quels supports les loggings seront-ils conservés ? Sur des disquettes au fonctionnement parfois aléatoire, sur des CD dont l'avenir apparaît incertain, sur des DVD, sur des bandes ? N'oublier pas que tous ces supports informatiques ont une durée de vie limitée (une centaine d'utilisation pour les bandes selon certains fournisseurs) ;
- où conservera-t-on les loggings ? Qui aura accès à ces loggings et selon quelle procédure ?
- sera-t-on sûr que les loggings ne pourront être modifiés ou manipulés ?

Toutes ces questions peuvent trouver une réponse et votre fournisseur informatique peut vous y aider.

Pistes d'action.
Un bon logging ne fera pas perdre de temps. En effet, il doit vous permettre de réagir par anomalie :

Exemples :

- *relevé de consultations anormalement élevé par un utilisateur ;*
- *tentatives répétées et infructueuses de connexion au programme sans autorisation ;*
- *relevé de copies de données ou de copies d'écran anormalement élevé ;*
- *tentative de connexion sous une autre identité ;*
- *nombre de modifications apportées à un dossier dépassant le nombre fixé par le service ;*
- *etc.*

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Norme 4.2.3.3. chaque CPAS connecté au réseau de la Banque Carrefour doit mettre en place un système de copie de sécurité (back up), régulièrement contrôlé, permettant de s'assurer, en cas de sinistre total ou partiel, qu'aucune perte de données irréparable ne puisse survenir (données nécessaires à l'application et à l'exécution de la sécurité sociale ainsi que celles concernant les applications et le système d'exploitation).

C'est en étroite collaboration avec la(les) personnes chargées de gérer le système informatique que le conseiller en sécurité de l'information du CPAS pourra veiller à la réalisation de cette tâche. Il s'agira, aussi bien pour les données nécessaires à l'application et à l'exécution de la sécurité sociale que celles concernant les applications et le système d'exploitation, de mettre en place un système de copie de sécurité régulièrement contrôlé (1). Ces copies de sécurité doivent permettre de s'assurer, en cas de sinistre total ou partiel, qu'aucune perte de données irréparable ne puisse survenir.
Pour assurer la sécurité des copies de sécurité, un exemplaire de celles-ci sera conservé dans un autre lieu.
Le conseiller en sécurité veillera à recevoir des équipes informatiques un document décrivant les procédures des sauvegardes et les procédures de restaurations qui y sont associées.
Ces documents seront imprimés et également conservés dans un autre lieu.

Le système de sauvegarde des données ("back-up") est nécessaire pour éviter une perte irréparable à la suite d'un accident. La sauvegarde doit permettre au CPAS de relancer ses activités après un incident qui aurait détruit le système en place.
Pour réaliser une sauvegarde, il suffit d'enregistrer les données sur un CD-rom, un DVD, une bande magnétique, etc. et de mettre cet enregistrement à l'abri. La sauvegarde des données doit se faire de manière automatique et régulière, idéalement chaque jour.

Idéalement, il y aurait lieu de procéder à une sauvegarde journalière limitée aux modifications des données de la journée du lundi au jeudi. Le vendredi, une sauvegarde des données et de la configuration informatique, c'est-à-dire une sauvegarde complète, sera réalisée.
Cette sauvegarde complète devrait être réalisée chaque semaine sur une bande différente pendant cinq semaines afin de pouvoir couvrir un mois. Ce système permet de restaurer des données historiques de paiement éventuellement utiles au CPAS.

Le schéma ci-dessous explique comment réaliser idéalement les sauvegardes.

Jour		Semaine 1		Semaine 2		Semaine 3		Semaine 4		Semaine 5		Semaine 1
Lundi	S1	Sauvegarde journalière	S5	Sauvegarde journalière	S1	Sauvegarde journalière	S5	Sauvegarde journalière	S1	Sauvegarde journalière	S5	Sauvegarde journalière
Mardi	S2	Sauvegarde journalière	S6	Sauvegarde journalière	S2	Sauvegarde journalière	S6	Sauvegarde journalière	S2	Sauvegarde journalière	S6	Sauvegarde journalière
Merc.	S3	Sauvegarde journalière	S7	Sauvegarde journalière	S3	Sauvegarde journalière	S7	Sauvegarde journalière	S3	Sauvegarde journalière	S7	Sauvegarde journalière
Jeudi	S4	Sauvegarde journalière	S8	Sauvegarde journalière	S4	Sauvegarde journalière	S8	Sauvegarde journalière	S4	Sauvegarde journalière	S8	Sauvegarde journalière
Vend.	T1	Sauvegarde totale	T2	Sauvegarde totale	T3	Sauvegarde totale	T4	Sauvegarde totale	T5	Sauvegarde totale	T1	Sauvegarde totale

Tableau 2.

Explications : le lundi de la première semaine, la bande S1 sert uniquement de back-up aux données modifiées ce lundi. Il en va de même jusqu'au jeudi.
Le vendredi de la semaine 1, une sauvegarde totale T1 (données complètes et système) est réalisée. Cette bande de sauvegarde est conservée à l'extérieur du CPAS.
La semaine 2, le même processus est répété. Chaque jour, une bande différente est utilisée.

Il y aura donc 8 bandes journalières de back-ups qui seront utilisées sur deux semaines. Le cycle se répétera ainsi toutes les deux semaines.
Quant aux sauvegardes hebdomadaires, les sauvegardes complètes (environnement informatique et données), elles seront étalées sur 5 semaines. Il y aura par conséquent 5 bandes (ou plus si la sauvegarde requiert plus de bandes) étalées sur un mois.

(1) Dans son plan de sécurité annuel, le conseiller doit prévoir au moins une fois par an un test de restauration de tout ou partie du système d'information à partir des supports de sauvegardes.

La détermination du cycle des sauvegardes doit être décidée par le responsable de la gestion journalière après consultation de toutes les parties impliquées : informaticiens, fournisseur, conseiller en sécurité et responsables des services internes.
Lors de cette discussion, il y a lieu d'évaluer la durée maximale admissible des données. Ainsi, si on conserve les données journalières au CPAS même, le responsable de la gestion journalière doit être prêt à accepter la perte de 4 jours de données, c'est-à-dire de travail. Si la sauvegarde hebdomadaire est conservée sur place, en cas de catastrophe importante, toutes les données seront détruites et il sera impossible au CPAS de récupérer quelque donnée que ce soit.

RECOMMANDATIONS EN MATIERE DE SAUVEGARDES

1. Généralités

En termes d'organisation, il est le plus souvent préférable de ne pas stocker des informations sur un PC. En ce qui concerne la confidentialité, il y a toujours le risque du vol du PC et en ce qui concerne la disponibilité, les sauvegardes (ou back-ups) seront plus régulièrement et systématiquement assurées par l'informatique.
Les sauvegardes sont des exemplaires de secours conservés sur une courte durée afin de pallier un accident, généralement informatique, et pour pouvoir restaurer ces données ou fichiers dans un état proche du dernier état connu.
Les archives sont des exemplaires de fichiers conservés sur une longue durée afin d'en garder une trace dans un état donné.
Il résulte de ces définitions que les buts ne sont pas les mêmes et que les informaticiens doivent disposer de règles précises et approuvées par le responsable de l'organisation, le responsable de l'application et le responsable informatique.
La responsabilité des sauvegardes des données stockées localement (sur le disque du PC ou de la station) incombe à chaque utilisateur.
Pour les postes connectés, une copie sur un serveur est recommandée, dans la mesure où des sauvegardes sont effectuées par l'administrateur du serveur et stockées de manière sécurisée.
Quand cela n'est pas possible, il est recommandé que les sauvegardes soient rangées dans une pièce différente du bureau dans lequel est situé le poste de travail (PC).
Les locaux de stockage des sauvegardes et des archives doivent être protégés.
Les fréquences et les exigences pour les sauvegardes et les restaurations doivent être définies.
Les loggings feront l'objet d'une procédure de sauvegarde quotidienne systématique.

2. Plans de sauvegardes des logiciels de base et des systèmes

Les sauvegardes des configurations sont conservées en dehors du site de production.
Une procédure permettant de s'assurer que la sauvegarde des configurations permet de reconstituer à tout moment l'environnement de production doit être mise en place.

3. Plans de sauvegardes des données applicatives

Voir tableau 2 des sauvegardes en page 27.

Le plan de sauvegarde doit être remis à jour à chaque changement de contexte d'exploitation et particulièrement à chaque création ou modification d'applications.
On doit contrôler régulièrement qu'une reprise ou un redémarrage est effectivement possible à partir des sauvegardes réalisées (test d'intégrité impromptu en réel).

4. Tests de bonne sauvegarde.
Il existe des systèmes testant la validité de la sauvegarde :
- *relecture d'une partie des données sur la bande de sauvegarde par le système ;*
- *réinstallation d'un échantillon de données pour les relire et vérifier leur validité.*

Si le système affiche l'information : 'La sauvegarde s'est bien déroulée", cela ne signifie pas que les données sont réutilisables. Assurez-vous qu'un système de test efficace vous garantisse la réutilisation de vos données. Votre fournisseur peut vous conseiller utilement.'

Comme pour l'ensemble des mesures de sécurité, l'installation des back-ups et leurs procédures doit répondre aux besoins spécifiques de chaque CPAS et être élaborée en conséquence.

Normes 4.2.3.4. chaque CPAS connecté au réseau de la Banque Carrefour doit installer un système et des procédures formelles et actualisées permettant de détecter des infractions à la sécurité, de les suivre et de les réparer.

Toute infraction à la sécurité dénonce une faiblesse dans les mécanismes mis en place, il est essentiel que ces incidents soient recensés et fassent l'objet de mesures correctives efficaces.
Les actions préventives sont essentielles dans ce contexte, notamment par :

- l'élaboration d'une politique stricte en matière des accès au système d'information (qui a droit à quoi) ;
- une rigueur dans les règles de définition du code utilisateur et de son mot de passe ;
- une rigueur dans la fréquence de la modification du mot de passe ;
- l'application d'un code de bonne conduite en matière de l'e-mail et de l'internet ;
- la mise en place et la publication d'une procédure à suivre en cas d'infection virale ;
- la mise à jour des antivirus et des firewalls ;
- l'abonnement (souvent gratuit) à des centres de compétences en matière d'informations sur l'évolution des attaques contre les réseaux ;

En cas d'incident une procédure formelle peut être un simple document transmis au responsable de la gestion journalière et rédigé, en fonction du type d'incident, par les différents acteurs responsables ou concernés au sein de l'organisation.

Cette procédure doit idéalement comprendre les éléments suivants :

- la description de l'infraction ou de l'incident ;
- l'origine ou la cause de l'infraction ou de l'incident ;
- les conséquences sur l'organisation et sur le réseau de la sécurité sociale ;
- les opérations effectuées pour remédier aux problèmes ;
- les personnes intervenues dans l'exécution des remèdes ;
- les actions a prendre pour palier l'infraction ou l'incident.

Voir Tableau 1.
Le rôle du conseiller est de veiller à la réalisation des actions correctives à entreprendre.

Comme pour l'ensemble des mesures de sécurité, installer un système et des procédures formelles et actualisées permettant de détecter des infractions à la sécurité, de les suivre et de les réparer doit répondre aux besoins spécifiques de chaque CPAS et être élaboré en conséquence.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Norme 4.2.3.5. **les CPAS connectés à la Banque Carrefour en mode APPC (message structurés) reprennent un numéro de programme dans la zone « Userid » de la partie préfixe du message qu'elle adresse à la Banque Carrefour bien qu'une personne physique soit à l'origine du message, la Banque Carrefour peut, a posteriori, retrouver le numéro de ce programme. La Banque carrefour ne connaît cependant pas l'identité de la personne physique qui a émis ce message.**

Dans ce cas, c'est donc au CPAS qu'il revient de faire la relation entre le numéro de programme qu'elle reprend dans la partie préfixe du message qu'elle adresse à la Banque Carrefour, et l'identité de la personne physique qui émet le message.

Pour faire le lien entre l'utilisateur et les consultations, le CPAS se réfère au système de loggings mis en place et décrit dans la norme 4.2.3.2.

D'autres renseignements peuvent être trouvés sur le site de la BCSS ;
http://ksz-bcss.fgov.be/documentation/fr/documentation/Flux%20de%20donn%E9es/CPAS/APPC%20F.pdf

Les CPAS connectés au réseau de la sécurité sociale via le site Web du SPP Intégration Sociale : sans objet.

Pour tout autre traitement informatisé de données sociales à caractère personnel implémenté au sein du CPAS, c'est au CPAS concerné qu'il appartient de saisir, de conserver et d'assurer la possibilité de consulter l'identité des utilisateurs, la date/heure ainsi que les données sociales à caractère personnel traitées.

Le conseiller lira attentivement le document détaillant l'ensemble des rôles et contraintes repris sur le site web de la BCSS :
http://ksz-bcss.fgov.be/documentation/fr/documentation/Flux%20de%20donn%E9es/CPAS/WEB%20F.pdf

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

4.2.4 Développement, production et maintenance des applications.

Norme 4.2.4.1. **chaque CPAS connecté au réseau de la Banque Carrefour doit disposer de procédures formelles et actualisées pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes afin d'éviter qu'une seule et même personne n'assure le contrôle de ce processus.**

La réalisation d'adaptations aux applications existantes ainsi que la mise en production de nouvelles applications doit toujours faire l'objet de tests préalables. Idéalement, ces tests sont réalisés dans un environnement autre que l'environnement de production (un environnement dédié à l'exécution de tests, sur des données fictives).
La mise en test et ensuite en production d'une application doit idéalement être réalisée par une personne différente. Cette procédure sera ensuite formalisée et adaptée au besoin.
Lorsqu'il s'agit d'une mise en production d'une nouvelle version pour une application existante, le processus de mise en production doit prévoir une sauvegarde de la version courante et de ses composants avant d'implanter la nouvelle version et ce afin de prévenir tous dysfonctionnements et de pouvoir revenir à la version précédente.

Attention : ceci n'est applicable qu'aux CPAS développant eux-mêmes leurs applications. Les CPAS sont toutefois libres de demander à leurs fournisseurs de respecter cette norme de sécurité.

Norme 4.2.4.2. chaque CPAS connecté au réseau de la Banque Carrefour doit disposer de procédures formelles et actualisées en vue d'élaborer la documentation lors du développement de nouvelles applications et systèmes et lors de la maintenance des applications et systèmes existants.

Pour les CPAS qui développent et actualisent leurs applications et systèmes, il s'avère utile qu'elles en établissent une documentation. Cette documentation pourra en préciser le développement et les modifications effectuées et permettra, à postériori, d'en connaître l'organisation.
Lors de l'installation de nouvelles applications, il s'agira également de veiller à la documentation/formation des utilisateurs, aux procédures de sauvegardes, aux contrôles des accès à l'application, à la présence, si nécessaire, des loggings d'utilisation , à l'intégration de cette application dans le plan de secours général.
Cette procédure sera ensuite formalisée et adaptée au besoin.

Comme pour l'ensemble des mesures de sécurité, disposer de procédures formelles et actualisées en vue d'élaborer la documentation lors du développement de nouvelles applications et systèmes et lors de la maintenance des applications et systèmes existants installer un système et des procédures formelles et actualisées permettant de détecter des infractions à la sécurité, de les suivre et de les réparer doit répondre aux besoins spécifiques de chaque CPAS et être élaboré en conséquence.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Attention : ceci n'est applicable qu'aux CPAS développant eux-mêmes leurs applications.

4.2.5 Protection du réseau.

Norme 4.2.5.1. chaque CPAS connecté au réseau de la Banque Carrefour doit limiter l'accès au(x) système(s) informatique(s) aux personnes/objets identifiés authentifiés et autorisés.

Par ''système informatique'', on entend les appareils et ordinateurs utilisés pour le traitement des données. Cette norme minimale de sécurité invite les CPAS, en fonction de l'importance de leur organisation, à protéger leur système informatique contre la malveillance et/ou le vol en instaurant des mesures conservatoires.

Par exemple : ces mesures, non limitatives, peuvent être énumérées comme suit :

- ne pas laisser le matériel informatique sans surveillance ;
- placer certains appareils importants dans un local sécurisé ;
- interdire le libre accès en dehors des heures de prestations (p. ex : porte du bureau fermée à clé, système de contrôle d'accès, détection intrusion, …) ;
- locker (verrouiller) les écrans ou forcer l'activation de screen saver ;
- imposer un système d'identification, d'authentification et d'autorisation d'accès au réseau ;
- localiser dans un endroit sécurisé les supports informatiques ;
- ne pas laisser traîner des documents imprimés contenant des informations confidentielles ;
- définir des procédures d'accompagnement ou de suivi lors des visites des fournisseurs de services informatiques ou autres ;
- changer les mots de passe des administrateurs systèmes après intervention des services techniques externes ;
- mettre en place et faire appliquer des règles de sécurité vis-à-vis des fournisseurs de service. (Police disponible sur le site de la BCSS).
- l'accès à distance (téléworking / homeworking) doit faire l'objet de mesures strictes. Des Polices sur le site de la BCSS précisent des règles en la matière. Nous conseillons aux CPAS concernées par cet usage de prendre contact avec le service de sécurité du SPP Intégration sociale qui pourra l'aider dans sa démarche.
- instituer un code de bonne conduite en matière d'utilisation de l'e-mail et de l'internet.

Comme pour l'ensemble des mesures de sécurité, les mesures pour limiter l'accès au(x) système(s) informatique(s) aux personnes/objets identifiés authentifiés et autorisés doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Norme 4.2.5.2. chaque CPAS connecté au réseau de la Banque Carrefour doit installer un système et des procédures formelles et actualisées permettant la détection, le suivi et la réparation d'infractions au niveau de la sécurité.

Identique à la norme 4.2.3.4 mais appliquée au réseau.

Norme 4.2.5.3. **les CPAS peuvent utiliser l'Extranet de la sécurité sociale pour les liaisons TCP/IP externes à la sécurité sociale.**

Pour leurs liaisons directes avec les réseaux TCP/IP externes à la sécurité sociale, les CPAS concernés doivent mettre en œuvre, des mesures de sécurité qui restent conformes aux mesures prises au niveau de l'Extranet de la sécurité sociale.

Cette norme n'est applicable qu'aux CPAS qui souhaitent avoir un accès à internet via l'extranet.

3.2.6. Plan de continuité.

Norme 4.2.6.1. chaque CPAS connecté au réseau de la Banque Carrefour doit réaliser une analyse des risques permettant l'élaboration d'un plan de continuité.

Le plan de continuité est un document rédigé par le conseiller en sécurité qui a pour objet de prévoir et d'exposer les actions à mener en cas d'incident.

Exemple: comment retrouver la connexion et les données après le vol du serveur ou sa destruction? Que faire en cas d'oubli ou perte des mots de passe? Comment réagir à une attaque de virus informatique?

1. L'analyse de risques

L'inventaire de l'ensemble des biens (bâtiment, locaux, matériels, logiciels, applications …) et des risques encourus (destruction, perte, malversation….) permet au conseiller en sécurité de savoir ce dont le CPAS doit disposer pour pouvoir fonctionner correctement.
En cas de catastrophe totale ou partielle, le CPAS devra tenter de recommencer à fonctionner le plus rapidement possible. Un délai sera déterminé lors d'une discussion entre le conseiller en sécurité et le responsable de la gestion journalière du CPAS. En effet, il se peut que toutes les activités ne soient pas prioritaires mais que d'autres doivent être redémarrées endéans un délai très court.
Le conseiller en sécurité devra alors réaliser une analyse des risques basée sur ce qui manquera au CPAS pour répondre aux exigences de redémarrage.
Les manques seront surtout constitués d'informations (quelle est la procédure pour refaire une connexion Publilink, comment redisposer d'un serveur rapidement pour redémarrer les activités et les paiements ? comment rediriger les lignes téléphoniques pour répondre aux demandeurs d'aide sociale ? où pourrons-nous nous réinstaller ? disposerons-nous des lignes téléphoniques et informatiques nécessaires ? etc.).
L'analyse de risque mettra, selon l'environnement du CPAS (environnement urbain ou rural, locaux disponibles ou non, taux de délinquance élevé ou non) l'accent sur les risques les plus probables. Le conseiller en sécurité pourra alors proposer un plan de continuité qui apportera une réponse adaptée à ces risques.

Pour ce fairfe, l'analyse de risques doit aborder particulièrement les aspects tels que :

- **les sinistres informatiques:** sont tous les problèmes logiques ou physiques qui touchent exclusivement un ou des éléments du système informatique du CPAS ;
- **les sinistres non informatiques en dehors des heures de bureaux:** sont des dommages causés au bâtiment, au personnel et au matériel suite à la réalisation d'une menace naturelle ou humaine.
- **les sinistres non informatiques pendant les heures de bureaux:** sont des dommages causés au bâtiment, au personnel et au matériel suite à la réalisation d'une menace naturelle ou humaine.
- **le plan de migration:** décrit le processus à suivre pour remettre en service le système informatique et fournir un environnement de travail pour le personnel. Il est important de préciser le rôle de chaque acteur concerné par ce processus de remise en service.

Il est évident que la catastrophe totale ne doit pas être seule prise en compte.

Norme 4.2.6.2. chaque CPAS connecté au réseau de la Banque Carrefour doit élaborer, tester et maintenir un plan de continuité afin de pouvoir garantir les missions de sécurité sociale du CPAS. En outre, il doit prévoir un centre de migration informatique en cas de sinistre partiel ou total.

Compte tenu des scénarii retenus dans l'analyse des risques, le conseiller en sécurité de l'information pourra, en étroite collaboration avec tous les acteurs de son organisation et en s'inspirant de la méthodologie décrite dans le document intitulé «Méthodologie commune pour l'élaboration d'un plan de continuité », établi par le groupe de travail « Sécurité de l'information », élaborer les mesures organisationnelles et technique nécessaires à la mise en place d'un plan de continuité.

D'une manière générale ce plan de continuité doit envisager des aspects tels que :

- **ressources humaines :** adresses, téléphones, autres coordonnées du personnel, des instances officiels, d'un comité de crise chargé de prendre les décisions suivant l'évolution de la situation, des fournisseurs informatiques et autres, des compagnies d'assurances, des téléphones utiles, de médecins, de partenaires professionnels..).
- **ressources techniques:** inventaire du matériel, des formulaires et support papier, de l'hardware, des softwares, de la structure du réseau informatique interne et externe, des applications, des processus de contact avec la presse, les partenaires….
- **plan de reprise technique**: description de toutes les étapes pour remettre en service et restaurer l'ensemble du système d'information.

En cas de survenance d'un sinistre, ce plan de continuité devra permettre au CPAS de s'assurer de la possibilité d'un redémarrage dans les meilleurs délais et de garantir la continuité des missions de sécurité sociale du CPAS.

Pour rester opérationnel, le plan de continuité sera testé régulièrement et actualisé en permanence. Sa documentation sera conservée en dehors de l'institution. (p. ex : les collaborateurs concernés conservent un exemplaire à leur domicile).
Des procédures doivent être prévues afin de disposer de ce plan en cas de sinistre.

Exemple : que se passerait-il si nos sauvegardes ne fonctionnent pas et que notre système informatique est détruit (inondation par exemple) ?

La norme 4.2.3.3 précise que le CPAS doit prendre des mesures visant à s'assurer qu'aucune perte de données irréparable ne puisse survenir. Le conseiller en sécurité veillera donc à proposer au responsable de la gestion journalière des mesures permettant de respecter cette norme.

En fonction des points qui ont été relevés dans l'analyse de risques, le conseiller en sécurité décrit dans le plan de continuité toutes les étapes à entreprendre en cas d'incident. Il est important que chaque personne qui est amenée à intervenir soit au courant des dispositions du plan de continuité, afin que même en absence du conseiller en sécurité, la connexion puisse être rapidement rétablie. La partie organisationnelle est donc très importante. Qui fera quoi, comment et où pour apporter une réponse et jouer son rôle ?

Reprenons l'exemple commencé ci-dessus: la destruction des sauvegardes et du système informatique.

Le conseiller en sécurité proposera donc une ou plusieurs des dispositions suivantes :

- un système de test garantissant la validité des back-ups ;
- une procédure comptant le nombre de back-ups pour remplacer les supports de sauvegarde (CD, DVD, bandes magnétiques, autres) à temps et éviter une détérioration de ceux-ci ;
- confier les sauvegardes à un fournisseur extérieur ;
- faire un double des back-ups ;
- acquérir un système de disques dur du type RAID ;
- etc.

Lorsqu'une solution aura été choisie, il faudra vérifier sa fonctionnalité et la tester, en interne ou avec le fournisseur. Elle sera alors utilisable si la catastrophe venait à se produire.
Naturellement, certains risques sont acceptables mais seule le responsable de la gestion journalière pourra en juger.
La destruction d'un PC, remplaçable rapidement, est un risque acceptable. La faillite d'un fournisseur peut être nettement plus grave. Que faire si celui-ci disparaît ? Qui va continuer à faire l'entretien de mon programme ? Comment puis-je le remplacer ? Quel est le risque que ce fournisseur tombe en faillite ?
Le conseiller en sécurité peut envisager de faire mettre une ''escrow clause'' dans le contrat avec le fournisseur. Cela implique que le fournisseur mette les sources actualisées de ses programmes en dépôt auprès d'un tiers de confiance : chambre de commerce, notaire, institution, autre afin que le CPAS puisse les récupérer et faire faire les maintenances en attendant de trouver une autre solution.

Comme pour l'ensemble des mesures de sécurité, les mesures visant à élaborer, tester et maintenir un plan de continuité afin de pouvoir garantir les missions de sécurité sociale du CPAS et prévoir un centre de migration informatique en cas de sinistre doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

4.2.6 Inventaire.

Norme 4.2.7.1. chaque CPAS connecté au réseau de la Banque Carrefour doit disposer d'un inventaire du matériel informatique et des logiciels qui est mis à jour en permanence.

Assurer la reconstruction dans les meilleurs délais et garantir ainsi la continuité des missions de sécurité sociale du CPAS implique d'élaborer, de tester et de maintenir un plan de continuité. Pour optimaliser son plan de continuité le conseiller en sécurité de l'information veillera, entres autres, à disposer d'un inventaire du matériel informatique et des logiciels mis à jour en permanence.
Cet inventaire peut être réalisé grâce à certains programmes. Pour obtenir plus d'informations, vous pouvez prendre contact avec le helpdesk du SPP Intégration sociale ou avec votre fournisseur informatique. L'inventaire des moyens nécessaires à l'exécution des tâches du CPAS pourra faire partie intégrante du plan de continuité du CPAS concerné. Cet inventaire devrait permettre, en cas de sinistre, d'assurer une reconstruction aussi rapide que possible du système informatique du CPAS.

Comme pour l'ensemble des mesures de sécurité, les mesures visant à disposer d'un inventaire du matériel informatique et des logiciels qui est mis à jour en permanence doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

4.2.7 Protection contre les infections par les virus informatiques.

Norme 4.2.8.1. chaque CPAS connecté au réseau de la Banque Carrefour doit disposer d'un manuel d'utilisation relatif à la prévention d'infections par les virus, au fonctionnement du logiciel antivirus installé et aux actions à entreprendre en cas d'infection par un virus.

Le conseiller en sécurité de l'information du CPAS veillera à la mise à disposition de ses utilisateurs d'un document (manuel) relatif au(x):

- mesures de prévention à respecter par les utilisateurs ;
- fonctionnement du logiciel antivirus éventuellement installé sur le poste de travail ;
- actions à entreprendre par l'utilisateur en cas d'infection (par exemple : l'action à entreprendre par un utilisateur peu parfois se limiter à : ne pas ouvrir un courrier électronique suspect et prévenir la personne chargée de la gestion du système informatique ou, en cas d'infection du PC par un virus : avertir la personne chargée de la gestion du système informatique).

Pour optimaliser l'élaboration de ce manuel une étroite collaboration avec la personne chargée de la gestion du système informatique s'impose.
Il faut bien entendu tenir compte des spécificités telles que l'antivirus utilisé.
Sur le site WEB de la BCSS vous trouverez une POLICE précisant les règles d'utilisation d'un poste de travail au sein d'une organisation de la sécurité sociale.

Nombre de CPAS peuvent aussi s'adresser à leur fournisseur de logiciel social qui s'occupe de leur antivirus ou de leur fournisseur d'accès comme VERA.

Comme pour l'ensemble des mesures de sécurité, les mesures à prendre en vue de disposer d'un manuel d'utilisation relatif à la prévention d'infections par les virus, au fonctionnement du logiciel antivirus installé et aux actions à entreprendre en cas d'infection par un virus *doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.*

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES

Norme 4.2.8.2. chaque CPAS connecté au réseau de la Banque Carrefour doit installer un logiciel antivirus actualisé afin de prévenir, de détecter et de corriger des infections par des virus informatiques.

Prémunir, détecter et corriger des infections du système informatique par des virus informatiques constitue l'un des défis actuels de toute organisation. Le conseiller en sécurité de l'information du CPAS veillera donc à ce qu'un logiciel antivirus soit adéquatement installé et actualisé aussi régulièrement que possible.
Le choix, l'installation ainsi que l'actualisation de ce logiciel ne peut être réalisé qu'en étroite collaboration avec la personne chargée de la gestion du système informatique du CPAS.
Pour avoir plus d'informations, vous pouvez contacter le helpdesk du SPP Intégration sociale.

Comme pour l'ensemble des mesures de sécurité, les mesures à prendre en vue d'installer un logiciel antivirus actualisé afin de prévenir, de détecter et de corriger des infections par des virus informatiques doivent répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Les éventuelles améliorations à y apporter peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

3.2.9. Surveillance / audit.

Norme 4.2.9. Chaque CPAS connecté au réseau de la Banque Carrefour doit organiser, au moins une fois tout les quatre ans, un audit concernant la situation de la sécurité tant au niveau logique que physique.

Les points d'attentions qui seront mis en évidence pendant l'audit seront signalés par le CPAS au groupe de travail Sécurité de l'information »

De plus, un résumé de l'audit effectué sera transmis au Comité Sectoriel de la sécurité sociale.

Après 6 mois, un rapport d'évaluation devra être communiqué au comité sectoriel de la sécurité sociale avec un aperçu des mesures prises entre temps. Les rapports originaux devront rester disponibles pour le Comité sectoriel de la sécurité sociale afin qu'il puisse les consulter en cas d'incident ultérieur.

Un audit a pour objectif de vérifier la réalité et l'efficacité des procédures mises en place pour prévenir un problème.
Un audit est une action positive dans le but d'aider l'organisation à évaluer un des composants de sa sécurité.
Une CPAS qui adhère au réseau de la BCSS est tenue de mettre en place ou de vérifier la présence de mesures nécessaires au respect des normes minimales de sécurité.
La mise en place d'un audit est une action concertée entre toutes les parties concernées sous la direction du responsable de la gestion journalière.
Un audit peut être réalisé par un membre, une équipe du CPAS autre que celle du conseiller en sécurité, un conseiller en sécurité d'un autre CPAS ou de la commune ou par une organisation externe (une société privée, une intercommunale agréee ou le service de sécurité spécialisé agréé). L'important est que l'auditeur dispose de suffisamment de recul et de compétence pour évaluer les domaines à contrôler.
L'objectif d'un audit est de surtout définir ou de proposer des lignes de conduite en vue de corriger si nécessaire la faiblesse. Dans ce contexte le rôle du conseiller soutenu par le responsable de la gestion journalière et de favoriser l'application des recommandations proposées.
Dans le plan de sécurité initial il sera proposé quelques pistes qui permettront d'identifier les priorités au sein de son organisation.

Exemple : l'audit de sécurité physique teste le bon fonctionnement du système d'intrusion. Une cascade de 3 numéros de téléphone a été prévue en cas d'effraction. L'audit montre que la première personne désignée était en vacances, que la deuxième est partie à la retraite et que la troisième a changé de numéro de téléphone.
La recommandation de l'audit sera de remettre la procédure à jour et de procéder au moins une fois par an à la vérification de l'actualité de la procédure et de la tester.

Comme pour l'ensemble des mesures de sécurité, l'organisation, au moins une fois tout les quatre ans, de l'audit concernant la situation de la sécurité tant au niveau logique que physique doit répondre aux besoins spécifiques de chaque CPAS et être élaborées en conséquence.

Les éventuelles mesures correctives à apporter suite à l'audit peuvent, avec l'accord de la personne chargée de la gestion journalière du CPAS, être inscrites dans le plan de sécurité du CPAS.

Coordonnées des participants

SPP Intégration sociale
G. Kempgens
Conseiller en sécurité
02.508.86.56
gilles.kempgens@mi-is.be

Helpdesk du SPP Intégration sociale
Helpdesk.security@mi-is.be
02.508.86.44 (fr)
02.509.83.48 (nl)

Cellule administratieve
M. M. Goffin
02.509.59.71
marcel.goffin@smals-mvm.be

Service de sécurité spécialisé agréé
Mr. J. Costrop
02.509.57.55
johan.costrop@smals-mvm.be

Banque Carrefour de la Sécurité sociale
Mr. Jean-Marie Gossiaux
Conseiller en sécurité
02.741.83.30
jean.marie.gossiaux@bcss.fgov.be

Service gestion de projet de la Banque Carrefour de la Sécurité sociale, service CPAS
Mr. Mark Stockx
02.741.84.85
mark.stockx@ksz.fgov.be

Helpdesk de la Banque Carrefour de la Sécurité sociale
02.741.83.11

VVSG
Chris Boens
Chris.boens@VVSG.be
http://www.vvsg.be/nl/werking_organisatie/ict_en_e-government/kruispuntbank_sociale_zekerheid.shtml

AVCB
Christian Lejour
Christian.lejour@avcb-vsgb.be

UVCW
Sébastien Lemaître
sebastien.lemaitre@uvcw.be

V-ICT-OR
security@v-ict-or.be

Kit de sécurité
GUIDE DE MISE EN PRATIQUE DES NORMES MINIMALES