# SESSION DE SECURITE DECEMBRE 2014

POD Maatschappelijke Integratie
SPP Intégration Sociale

# INDEX

# NOUVELLES NORMES

## 15.1 Collaboration avec des sous - traitants.

- Dans le cadre d'une solution de type « Cloud Computing », la politique de sécurité y relative (ISMS.0050) précise que le choix dans une telle situation est limité uniquement à des services cloud « communautaire[16] » (ou « privé »).

16 Infrastructure partagée par plusieurs organisations qui ont des intérêts communs ou des contraintes (légales,...) identiques.

# NOUVELLES NORMES

## 7.2 Tout CPAS doit sensibiliser chaque collaborateur à la sécurité de l'information.

**Différents moyens (campagne d'affichage, formation spécifique, ...) peuvent être utilisés en fonction du « profil » de chacun.**

# NOUVELLES NORMES

## 11.4 Mise au rebut ou recyclage sécurisé du matériel.

**Tout CPAS doit:**

- **prendre des mesures pour que toute donnée soit supprimée ou rendue inaccessible sur tout support de stockage avant sa mise au rebut ou recyclage.**

# NOUVELLES NORMES

## 12.1 Séparation des environnements

**Tout CPAS doit:**

- **prendre les mesures adéquates pour que l'environnement de production soit séparé et distinct des autres environnements tels : développement, acceptation, test…**

# NOUVELLES NORMES

## 12.1 Séparation des environnements

**Tout CPAS doit:**

- **s'assurer que tout développement, ou test soit exclu au sein de l'environnement de production. Dans certains cas de figure, cas exceptionnel, ces tests peuvent déroger à la règle moyennant la mise en place de mesures adéquates.**

# NOUVELLES NORMES

## 8.4 Support physique en transit.

**Tout CPAS doit prendre les mesures nécessaires pour protéger, contre les accès non autorisés, les supports en transit dont notamment les backups contenant des données sensibles.**

# NOUVELLES NORMES

## 9.4 Utilisation des services en réseau

**Tout CPAS doit prendre les mesures adéquates afin que toute personne n'ait uniquement accès qu'aux services pour lesquels elle a spécifiquement reçu une autorisation.**

# NOUVELLES NORMES

## 14.4 Sécurité applicative

**Tout CPAS doit:**

- **prendre les mesures nécessaires pour assurer la sécurité au niveau applicatif dans le but de minimiser les brèches potentielles de sécurité (confidentialité, intégrité, disponibilité).[14]**

**14: liés aux menaces existantes telles que SQL injection, Spoofing, Cross Site Scripting, Elevation Privilege (Top Ten OWASP: *Open Web Application Security Project*)**

# NOUVELLES NORMES

## QUESTIONS ?

# NORMES REVISEES

**7.1 Tout CPAS doit mettre en place une procédure garantissant que tous les collaborateurs internes et externes s'engagent à respecter leurs obligations en ce qui concerne la confidentialité et la sécurité des données.**



# 13.2.1 Cartographie des flux de l'extranet

**Tout CPAS doit:**

- **tenir à jour une cartographie technique[13] des flux implémentés au travers de l'Extranet de la sécurité sociale et en informer le conseiller en sécurité.**

**[13] Nécessaire à la gestion des firewalls dans les différentes zones de l'Extranet. Pour les CPAS qui travaillent avec une maison de soft, cette cartographie est tenue à jour par la maison de soft.**



# 12.4 Politique de sauvegarde

## Afin d'éviter la perte irréparable de données toute organisation doit :

- définir la politique et la stratégie organisant la mise en œuvre d'un système de sauvegarde en phase avec la gestion de la continuité (norme 17).

- contrôler régulièrement les sauvegardes réalisées dans ce cadre.



# 12.6 Traçabilité des identités.

- Chaque CPAS participant à la transmission de données au travers de la Banque Carrefour est tenu d'assurer à son niveau la traçabilité des identifiants utilisés.

- Cette traçabilité doit permettre l'identification de bout en bout des identifiants utilisés.

# NORMES REVISEES

## 17.1 Gestion de la continuité.

**Tout CPAS doit:**

- **élaborer, tester et maintenir un plan de continuité basé sur une analyse des risques, afin d'assurer la mission de l'organisation dans le cadre de la sécurité sociale.**

# NORMES REVISEES

## 18.1 Audit externe

## Tout CPAS doit:

- **entreprendre périodiquement un audit de conformité relatif à la situation de la sécurité telle que circonscrite par les normes minimales.**

**Rappel: effort financier et délai de 5 ans.**

# NORMES REVISEES

## QUESTIONS ?

# CHAMPS D'APPLICATION

**Il serait de bon usage que ces normes s'appliquent également à la sécurité de l'information au sens large du terme, telle que définie dans l'AR du 17/03/13 relatif aux conseillers en sécurité institués par la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral ...**

# CHAMPS D'APPLICATION

**...et comme reprise dans l'AR du 12/08/93 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale:**

**« stratégie, règle, procédures et moyens de protection de tout type d'information tant dans les systèmes de transmission que dans les systèmes de traitement en vue de garantir la confidentialité, la disponibilité, l'intégrité, la fiabilité, l'authenticité et l'irréfutabilité de l'information ».**

# NOUVELLES NORMES

## QUESTIONS ?

# NORMES REVISEES

## 16.1 Incidents majeurs (I)

**Tout CPAS doit:**

- **veiller à ce que le service de Sécurité de l'information soit informé, par le service responsable, des incidents majeurs susceptibles de compromettre la sécurité de l'information et des mesures prises pour faire face à ces incidents.**

# 16. Gestion d'incidents relatifs à la sécurité de l'information

## 16.1 Incidents majeurs[17] (II).

**Tout CPAS doit:**

- **s'assurer que la BCSS soit informée de tout incident de sécurité classifié "Majeur" suivant la politique générale de remontée d'incident sécurité établie au sein de la sécurité sociale[18].**

# NORMES REVISEES

17 **Incidents majeurs : Il est souhaitable que toute organisation définisse le caractère « majeur » d'un incident. Par exemple, Incendie, dégâts causés par l'eau, attaque de codes nocifs, tentatives d'intrusion (logique ou physique), vol ou perte d'ordinateurs portables, interruption des loggings peuvent être considérés comme des incidents majeurs.**

18 **Cette norme ne sera d'application qu'à partir du moment où la politique sécurité relative à la remontée d'incident sécurité au sein de la sécurité sociale sera disponible et validé.**

# NOUVELLES NORMES

## QUESTIONS ?

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Le gestionnaire de sécurité principal assume les tâches suivantes :

- saisir les demandes relatives aux utilisateurs ;
- créer l'utilisateur sur le portail fédéral le cas échéant ;
- assurer la liaison avec l'ensemble des gestionnaires et contacts de sécurité ;

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Le gestionnaire de sécurité principal assume les tâches suivantes :

- définir les institutions (agences et départements) dans le système de gestion des utilisateurs en collaboration avec P&O et la BCE (pour créer le numéro BCE) ;
- définir les gestionnaires et contacts de sécurité dans le système de gestion des utilisateurs.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

La Commission de la vie privée recommande dans son document "Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" la désignation d'un conseiller en sécurité au sein de l'organisme.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

La loi du 8/08/83 organisant un registre national des personnes physiques prévoit la mise en place d'un consultant en sécurité dans chaque autorité publique, organisme public ou privé qui a obtenu l'accès aux informations du RN.

L'identité de ce consultant en sécurité doit être communiquée au comité sectoriel du Registre national.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Le Gestionnaire Local est désigné par le Responsable Accès Entité (ou Co-Responsable Accès Entité) pour assurer la gestion d'une qualité (i.e. domaine d'activité) d'une entreprise/ organisation.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

- Les tâches du gestionnaire local sont :
  - désigner un ou plusieurs Co-Gestionnaires Locaux pour le seconder ;
  - bloquer, débloquer ou supprimer les Co-Gestionnaires Locaux au sein de sa qualité (cette fonctionnalité n'est pas accessible aux Co-Gestionnaires Locaux);
  - gérer les subdivisions pour autant que cette qualité l'y autorise
    - ajouter/supprimer une subdivision, libre ou sous contrainte en fonction des possibilités qui lui sontdonnées, et y associer certaines applications ;
    - bloquer/débloquer une subdivision ;
      gérer les (Co-) Gestionnaires Subdivision.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

- gérer des Utilisateurs au sein de la qualité qu'il gère :
  - enregistrer un nouvel Utilisateur ;
  - attribuer des autorisations aux Utilisateurs qu'il gère ;
  - changer certains attributs des Utilisateurs (choix linguistique, e-mails et accès aux applications) ;
  - bloquer, débloquer et supprimer des Utilisateurs.
- rechercher et sélectionner des Utilisateurs au sein du domaine d'activité qu'il gère ;
- désigner un Utilisateur technique qui sera la personne de contact pour tout ce qui concerne l'envoi de données par traitement batch (messages structurés) ;
- consulter les informations spécifiques à la qualité (et définir une adresse e-mail pour cette qualité).

# EXERCICE D'INTEGRATION CPAS - COMMUNES

**Les normes minimales de sécurité s'appliquent aux institutions de sécurité sociale.**

**Etant donné que les communes sont connectées au Registre national, les principes de sécurité dérivant de la loi "vie privée" s'appliquent à celles-ci.**

# EXERCICE D'INTEGRATION CPAS - COMMUNES

**Les référentiels de sécurité établis par la Commission de la Protection de la Vie Privée s'appliquent en l'espèce.**

**Les administrations communales doivent désigner un conseiller en sécurité et disposer d'une politique de sécurité. La communication de données à caractère personnel par les communes requiert l'autorisation préalable de la section compétente de la Commission de la Protection de la Vie Privée.**

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Toute collaboration entre l'administration communale et le CPAS permettant d'aboutir à une meilleure intégration des services au citoyen et à une meilleure efficacité et efficience pour les parties concernées doit être pleinement soutenue. Cette collaboration ne peut cependant pas porter atteinte aux 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* ou aux autres dispositions pertinentes relatives à la protection de données (à caractère personnel).

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Ils s'acquittent de cette tâche de manière distincte en développant leur propre politique en matière de sécurité de l'information et en effectuant tous les contrôles nécessaires à cet égard.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

La collaboration entre ces 2 organisations, par exemple en faisant appel aux mêmes membres du personnel et à la même infrastructure, est autorisée pour autant que chacune d'entre-elles respecte ses obligations et contraintes inhérentes à leurs domaines d'activités respectifs.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Lors de l'utilisation d'une infrastructure informatique commune, il y a lieu de veiller à ce que les mesures techniques et organisationnelles nécessaires soient appliquées de sorte que seules les personnes autorisées aient accès aux données à caractère personnel nécessaires à l'exercice de leurs missions.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Lors de l'accès aux données, il y a obligation d'en identifier formellement son auteur.

Des droits d'accès aux données à caractère personnel **distincts** doivent être définis pour chaque utilisateur en fonction de son rôle et de l'organisation pour laquelle il travaille.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Une autorisation du comité sectoriel portant sur l'échange de données à caractère personnel entre la commune et le centre public d'aide sociale est requise.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

L'utilisation de logiciels communs est autorisée, à la condition que lors de l'accès à ceux-ci et aux données y enregistrées, il puisse être précisé au nom de quel organisation (commune ou CPAS) l'accès a été réalisé. Il y a également lieu de prévoir une séparation logique pour le traitement des données.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

**Services communs concernés:**

- **service du personnel;**
- **service comptable;**
- **accueil;**
- **service logistique;**
- **service informatique (niveau de sécurité le plus élevé: traçabilité exigée).**

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Fichier d'adresses commun

Tout échange de données à caractère personnel social doit être autorisé par le Comité Sectoriel de la sécurité sociale et de la santé, et doit avoir lieu à travers la Banque Carrefour de la sécurité sociale.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

De ce fait, le fichier d'adresses commun ne peut contenir de données personnelles sociales, sans autorisation accordée par le Comité Sectoriel.

Donc, le traitement de ce genre de fichiers est soumis au respect de la "Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel".

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## "Porteunique"

- Par ce terme de "porte unique", on définit le concept que dans un même lieu, espace, plusieurs services communaux accessibles aux citoyens implémentent leurs guichets, tel que (liste non exhaustive) :
  - service population;
  - service état civil;
  - centre public d'aide sociale;
  - agence locale pour l'emploi;
  - logement social;
  - service de Police locale; -...

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Cette initiative est autorisée pour autant que les mesures décrites[1] soient respectées par l'ensemble des organisations qui implémenteront un guichet.

1 Cf https://www.bcss.fgov.be/binaries/documentation/fr/securite/policies/isms_043_ocmw_cpas_gemeente_commune_fr.pdf

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Mise en commun des technologies de l'information

- Mise en commun autorisée selon les normes et règles de chaque organisation.
- Mais d'abord, un accord de coopération devra être conclu entre les différentes organisations partenaires.
- Cet accord devra mentionner les compétences de chaque organisation, ainsi que ses responsabilités.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Si une partie de cette gestion est confiée à un sous-traitant, il est impératif que celui-ci soit lié à l'organisation par un contrat qui mentionnera ses obligations en matière de confidentialité ainsi que de protection des données à caractère personnel, tel que définies dans la "Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel"

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Sauvegardes

Si les supports quittent l'institution, le contenu doit être chiffré.

Si les supports contiennent les données des 2 institutions, des mesures de chiffrement devront être mises en place de manière à ce que chaque organisation soit uniquement autorisée à lire ses propres données.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

**L'accès à ces supports de sauvegardes doit être octroyé aux personnes habilitées, selon la nécessité. La traçabilité des accès doit être garantie.**



## Accès à internet et utilisation de messagerie électronique

Des collaborateurs employés par plusieurs organisations devront disposer d'une adresse de messagerie électronique au sein de chacune d'elles.



## Droits d'administrateur pour les utilisateurs ordinaires

Afin d'assurer une sécurité optimale du réseau, un utilisateur ordinaire ne pourra pas disposer des droits "administrateur" sur son poste de travail.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Cette mesure doit aussi bien s'appliquer sur les postes de travail fixes que sur les postes de travail mobiles en sachant que dans le cas de nouvelles technologies (smartphones, tablettes,...) une analyse de risque doit être effectuée de manière à appliquer les mesures de protection adéquates.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

**Chaque accès à un système d'information contenant des données à caractère personnel doit pouvoir être tracé, de manière à pouvoir répondre aux questions "Qui, quand, quoi, comment".**

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Il doit donc être possible d'attribuer à un utilisateur **seulement** les droits nécessaires à l'accomplissement de sa mission.



## Traces de sécurité

L'intégrité et la confidentialité de ces traces de sécurité doivent être garanties et elles ne doivent être consultables que par l'autorité compétente.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Séparation des organisations

Même en cas de collaboration entre différentes organisations, il est nécessaire qu'une séparation physique ou logique soit établie entre celles-ci..

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## Séparation des organisations

- Au niveau réseau, si une séparation physique n'est pas possible, une séparation logique devra être mise en place de manière à ce que chaque utilisateur ait uniquement accès à ses propres ressources.
- Au niveau système d'exploitation, les organisations doivent être logiquement séparées (Org. Unit par exemple).



# Liaison entre différents sites.

Lorsque la ou les organisations sont reparties sur plusieurs sites, il y a lieu de prendre les mesures nécessaires afin que la liaison entre ceux-ci présente une sécurisation optimale.



# Liaison entre différents sites.

A cette fin, plusieurs possibilités existent :

- une solution consiste en une ligne directe (virtuelle) entre les différents sites.
- une autre solution consiste en l'installation d'une liaison sans fil uniquement entre les deux sites. Cf la politique de sécurité de la BCSS.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

Une autre solution consiste en la mise en place d'un VPN entre les sites, via l'internet. Afin de garantir la sécurité des échanges, les mesures de sécurité adaptées devront être mises en place. La solution standard recommandée par la Banque Carrefour est la mise en place d'une solution VPN "IPsec" LAN-to-LAN.

# EXERCICE D'INTEGRATION CPAS - COMMUNES

## QUESTIONS ?

# NOUVELLES NORMES

**FIN**