PRESENTATION DU QUESTIONNAIRE DES NORMES MINIMALES DE 2019

ANNEE 2018

NAMUR (BEEZ) SEPTEMBRE 2019
GILLES KEMPGENS

Questionnaire 2019 pour l'évaluation des normes minimales : année contrôlée 2018

Cadre

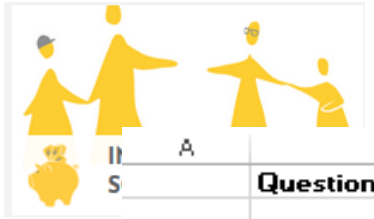
Les normes minimales de sécurité publiées sur le site de la Banque Carrefour de la Sécurité Sociale s'appliquent en premier lieu aux institutions de sécurité sociale, comme mentionné à l'article 2, paragraphe 1, 2°, de la loi du 15 janvier 1990 portant sur la création et l'organisation d'une Banque Carrefour de la Sécurité Sociale. Elles s'appliquent également aux organismes qui ont adhéré au réseau de la sécurité sociale en vertu de l'article 18 de cette loi (voir les arrêtés royaux des 16 janvier 2002, 15 octobre 2004 et 4 mars 2005 - à consulter sur https://www.ksz-bcss.fgov.be/fr sous la rubrique "législation" et la rubrique "réseau du BCSS"). Enfin, elles s'appliquent également à certaines organisations qui ont été explicitement désignées à cette fin par le comité sectoriel de sécurité sociale et de santé ou par le comité de sécurité de l'information, à la suite d'une délibération concernant le traitement des données à caractère personnel provenant du réseau de sécurité sociale (le respect des normes minimales de sécurité est dans certaines délibérations une condition essentielle du traitement des données personnelles).

But

Ce questionnaire a pour but d'évaluer et de déterminer si les normes de sécurité en vigueur au sein de l'organisation sont en ligne avec les objectifs des normes minimales de sécurité, tout en tenant compte de leur situation spécifique et de l'importance des moyens de fonctionnement à protéger.

La vérification des normes minimales de sécurité auprès de tiers qui traitent' des données sociales à caractère personnel pour le compte d'une organisation, relève de la responsabilité du responsable du traitement ou donc de l'organisation qui confie des travaux à des tiers. (Règles RGPD - Article 28) .

Intro | Context | Questionnaire | LIEN ISO | Groupe



	A	B	C	I
		Question	**Réponse**	
Question 1		Le CPAS gère-t-il ses propres systèmes critiques ?	Oui	Cela signifie que le CPAS est le propriétaire de son réseau et de son OS.
Question 2		L'organisation appartient-elle au réseau primaire de sécurité sociale ?	Non	Aucun CPAS n'appartient au réseau primaire La réponse est donc toujours : "Non".
Question 3		L'organisation dispose-t-elle de médias mobiles ?	Oui	Le CPAS utilise-t-il des disques durs portables, des clefs USB, des CD, etc. ?
Question 4		L'organisation dispose-t-elle d'appareils mobiles ?	Oui	Le CPAS utilise-t-il des PC portables, des smartphones et/ou des tablettes ?
Question 5		L'organisation fait-elle appel à un tiers pour gérer ses systèmes ?	Oui	Le CPAS travaille-t-il avec des fournisseurs informatiques extérieurs ?
Question 6		L'organisation utilise-t-elle une solution de cloud pour gérer ses systèmes, y compris ceux de tiers qui hébergent des applications dans leur datacenter ?	Oui	Le CPAS travaille-t-il avec des clouds extérieurs dont Office 365 de Microsft, Dropbox,
Question 7		L'organisation utilise-t-elle le wifi pour accéder à ses propres systèmes informatiques ?	Non	
Question 8		Le CPAS est-il une institution de gestion de réseau secondaire ?	Non	La réponse est toujours : "Non".
Question 9		Les employés peuvent-ils faire du télétravail ?	Non	Le personnel du CPAS peut-il travailler à domicile ?
Question 1(		Le CPAS utilise-t-il la cryptographie en régie ?	Oui	Le CPAS utilise-t-il des services de cryptographie pour ses données ou back-ups ?
Question 1		Les systèmes d'information ICT (applications) sont-ils achetés ?	Oui	Les applications (sociales, comptables, autres) sont-elles fournies et entretenues par des société extérieures ?
Question 1		Les systèmes d'information ICT (applications) sont-ils fournis et entretenus par des parties externes ?	Oui	Les applications (sociales, comptables, autres) sont-elles fournies (leasing par exemple) par s société extérieures ?
Question 1		Les systèmes d'information ICT (applications) sont-ils développés en interne ?	Non	Des applications informatiques, routines, logiciels sont-ils développées en interne par le CPAS lui-même ?
		Vous pouvez maintenant commencer à répondre aux questions du questionnaire sur la sheet suivante.		

Questionnaire 2019 pour l'évaluation des normes minimales : année contrôlée 2018

Nom de l'institution **(obligatoire)**	Nom du Adresse : Numéro d'entreprise (BCE) :	
Prénom, nom et courriel du délégué à la protection des données (DPD) (obligatoire)		
Prénom, nom et courriel du délégué à la protection des données adjoint (DPD adjoint) (facultatif)		
Prénom, nom et courriel de la personne chargée de la gestion journalière de l'institution **(obligatoire)**		

Nr. question	BLD	Norm	Question	Réponse	Argumentez si non	Explication
A			**Politique de sécurité de l'information et principes de base**			
			Cette politique vérifie si l'organisation dispose d'une politique de sécurité de l'information.			
1	BLD KERN	5.1.1	Le CPAS a-t-il intégré les principes clés dans sa sécurité de l'information ?			Cf la politique de sécurité suivante contenant les principes-clef: https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_kern_pri
2	BLD KERN	5.2.1	Le CPAS dispose-t-il d'une politique de sécurité de l'information formelle et actualisée, approuvée par le responsable de la gestion journalière ?	Oui Non NA		La politique de sécurité de l'information est un instrument de management destiné à soutenir l'application de la sécurité dans le CPAS. Cf l'exemple de politique de sécurité disponible ici: https://www.mi-is.be/sites/default/files/documents/exemple_politique_de_securite_2016.do

1 = numéro de la question
2 = chapitre de sécurité abordé dans les questions
3 = cliquer ici pour répondre
4 = explication complémentaire fournie par le SPP Intégration sociale

A	B	C	D	E	F	P
B			**Plan de sécurité et la gestion des risques**			
			Ceci vérifie si l'organisation dispose d'un plan de sécurité de l'information et a libéré les crédits de fonctionnement et les ressources nécessaires en vue de son exécution.			
3	BLD HR	5.3.1.2c	Le CPAS dispose-t-il d'un plan de sécurité de l'information approuvé par le responsable de la gestion journalière ?			Le plan de sécurité est consitué du rapport annuel de sécurité et du plan triennal de sécurité révisable annuellement. Des exemplaires de ces rapport - plan sont disponibles sur le site du SPP IS: https://www.mi-is.be/sites/default/files/documents/rapport_securite_annuel_v2_0.doc et https://www.mi-
			Ceci vérifie si la gestion des risques est axée sur la sécurité, la vie privée et est conforme au RGPD.			
4	BLD RISK	5.2.2a	Le CPAS dispose-t-il d'un processus d'évaluation des risques (utilisé dans le cadre des projets et des processus) qui tient compte de la sécurité de l'information et de la vie privée ?			Ce processus est une méthodologie d'évaluation de risque. Le CPAS choisit librement la méthodologie qu'il souhaite.
5	BLD RISK	5.2.2b	Le CPAS a-t-il communiqué toutes les évaluations de risques contenant un risque résiduel majeur à la direction ?			Existe-t-il une évaluation des risques pour le bon fonctionnement du CPAS ? Si oui, cette liste contient-elle un ou des risques susceptibles de survenir et de nuire gravement pour le fonctionnement du CPAS ?
6	BLD RISK	5.2.2c	Le CPAS dispose-t-il pour son évaluation des risques les principes énumérés dans la « directive relative à l'évaluation des risques » (annexe C de la politique « Evaluation des risques ») ?			Cf https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_risk_evaluation_risques.pdf
C			**Organisation de la sécurité de l'information**			
			Ceci vérifie si l'organisation dispose d'un service de sécurité de l'information.			
7		5.3.1.2a	Existe-t-il un service chargé de la sécurité de l'information placé sous l'autorité fonctionnelle directe du Directeur général/directrice générale de l'organisation ?			

8	BLD HR	5.3.1.2a	Le CPAS dispose-t-il, en son sein, d'un service de sécurité sous la direction du délégué à la protection des données (DPD) ?			
9	BLD HR	5.3.1.2b	Le CPAS a-t-il communiqué l'identité de son délégué à la protection des données (DPD) et de ses adjoints éventuels à la Banque Carrefour ou, en ce qui concerne les CPAS, au SPP Intégration sociale ?			
10	BLD HR	5.3.1.2d	LE CPAS qui est raccordé au réseau de la Banque Carrefour dispose-t-il des moyens de fonctionnement utiles (ressources, outils, ...) y compris un plan de sécurité de sorte que le service de sécurité et/ou le délégué à la protection des données (DPD) puisse réaliser les tâches qui lui sont confiées ?			Le DPD et son service de sécurité éventuel disposent-ils des moyens suffisants (ressources financières, formations, budget) pour garantir leyr bon fonctionnement ?
11	BLD HR	5.3.1.2f	Le CPAS dispose-t-il de procédures pour la communication d'informations au délégué à la protection des données (DPD) de sorte que ce dernier dispose des données lui permettant d'exécuter la mission de sécurité qui lui a été confiée ?			Existe-t-il une procédure officielle connue de tous pour communiquer au DPD les informations nécessaires à l'exécution de sa fonction ?
12	BLD HR	5.3.1.3	Le CPAS dispose-t-elle d'une plateforme de décision pour valider et approuver les mesures de sécurité ?	NA	Chaque CPAS a un Conseil de l'Action Sociale qui constitue une plateforme de décision. Il est cependant possible que les grands	
			Vérifie l'échange d'informations pertinentes entre l'organisme de gestion et le réseau secondaire.			
13	BLD HR	5.3.1.4	L'organisation gérant un « réseau secondaire » organise-t-elle avec les organisations faisant partie de son réseau, au moins une fois par semestre, une réunion du sous-groupe de travail « Sécurité de l'information » ?	NA		

14	BLD HR	5.3.1.4	Si vous êtes une organisation faisant partie d'un « réseau secondaire », assistez-vous aux sessions de sécurité qui sont organisées au moins une fois par semestre par le SPP Intégration sociale» dans le cadre du sous-groupe de travail « Sécurité de l'information » ?			Il s'agit ici des sessions de sécurité annuelles organisées par le SPP IS ou de ses sessions de formation en sécurité, RGPD, autre.
D			**Sécurité liée aux collaborateurs**			
			Ceci vérifie si l'organisation dispose d'une politique relative à la sécurité de l'information et à la vie privée qui est adaptée aux collaborateurs.			
15	BLD CLEAR	5.4.2a	Le CPAS dispose-t-il d'une politique indiquant que la collaboration de l'ensemble des collaborateurs est essentielle pour la sécurité de l'information et la vie privée ?			Cette politique est soit la politique de sécurité dans laquelle est mentionnée l'importance de la collaboration et de la confidentialité, soit le règlement du personnel qui contient les mêmes clauses.
16	BLD CLEAR	5.4.2b	Le CPAS dispose-t-il d'une politique indiquant que l'utilisateur demeure responsable des informations, quelle que soit la forme sous laquelle ces informations sont enregistrées ?			Existe-t-il une mention spécifique dans le règlement du personnel ou dans la politique de sécurité rappelant la responsabilité des utilisateurs en matière de gestion des informations ?
17	BLD INCID	5.13.1b	Le CPAS a-t-il signé un contrat avec les collaborateurs dans lequel il est stipulé que tout collaborateur (fixe ou temporaire, interne ou externe) est obligé de signaler tout accès, utilisation, modification, publication, perte ou destruction non autorisé d'informations et de systèmes d'information ?			
18	BLD HR	5.3.1.1	Le CPAS réalise-t-il les activités obligatoires (si d'application) avant, pendant et lors de la cessation ou modification du contrat de travail telles que décrites dans les normes minimales 5.3.1.1 ?			
19	BLD CLEAR	5.4.1	Le CPAS sensibilise-t-il annuellement tout collaborateur à la sécurité de l'information et à la vie privée ?			Organise-t-on régulièrement des campagnes de sensibilisation à la sécurité ?

20	BLD MOBILE	5.3.2.1g	Le CPAS sensibilise-t-il régulièrement les utilisateurs concernant les bonnes pratiques d'utilisation et leurs responsabilités (en particulier en ce qui concerne la connexion à des réseaux sans fil publics) ?			Idem mais en matière de connexion à un réseau sans fil. L'utilisateur vérifie-t-il toujours que le réseau wifi mentionné (celui du CPAS par exemple) est bien celui qui est annoncé ?
21	BLD CLEAR	5.4.1	Réalise-t-il annuellement une évaluation du respect de cette politique dans la pratique (au moyen d'une enquête interne) ?			
22	BLD COMPLY BLD HR	5.15.1d	Le CPAS dispose-t-il d'une procédure disciplinaire formelle pour les travailleurs ayant commis une infraction à la sécurité de l'information ou à la vie privée ?			Le règlement du personnel prévoit-il explicitement des sanctions en cas d'infraction à la sécurité ?
E			**Sécurité physique et protection de l'environnement**			
			Cette politique vérifie si l'organisation dispose d'une politique relative à la limitation de l'accès physique.			
23	BLD CLEAR	5.8.1	Le CPAS prend-il les mesures nécessaires permettant de limiter l'accès aux bâtiments et locaux aux personnes autorisées et effectue-t-elle un contrôle à ce sujet tant pendant qu'en dehors des heures de travail ?			Les accès aux locaux sont-ils contrôlés (contrôle d'accès) et les visiteurs ne peuvent -ils avoir accès aux archives, aux documents et aux systèmes informatiques sans contrôle ?
F			**Protection de l'accès logique à systèmes d'information (production, test, development, …)**			
			Cette politique vérifie si l'organisation dispose d'une politique relative à la limitation de l'accès logique.			
24	BLD CLEAR	5.4.2c	Le CPAS a-t-il sécurisé l'accès à l'information par un dispositif d'accès précis et a-t-il implémenté un système d'accès logique afin d'éviter tout accès non autorisé à l'information de l'organisation ?			Y a-t-il un nom d'utilisateur et un mot de passe distinct pour chaque utilisateur lorsqu'il a accès au(x) réseau(x) du CPAS (CPAS, maison de repos, antennes extérieures, etc.) ?
25	(BLD APPDEV)	5.6.6	Le CPAS a-t-il pris les mesures adéquates afin que toute personne ait uniquement accès aux services pour lesquels elle a spécifiquement reçu une autorisation ?			Chaque utilisateur a-t-il accès uniquement aux applications auxquelles il doit avoir accès (et pas aux applications qui ne lui sont pas destinées, exemple: CPAS - commune).

26	BLD APPDEV	5.11.2a	L'ensemble des collaborateurs (interne et externe) travaillent-ils avec des moyens ICT (mis à la disposition par l'organisation) sur la base d'une autorisation minimale pour l'exécution de leurs tâches ?			Chaque utilisateur, qu'il soit interne ou externe, ayant accès au réseau ou à des applications du CPAS a-t-il bien reçu une autorisation minimale spécifique (mot de passe, autorisation nominative enregistrée) ?
27	BLD APPDEV BLD ETHICS	5.6.5	Le CPAS a-t-il limité l'accès du/des système(s) informatique(s) aux gestionnaires d'information identifiés, authentifiés et autorisés ?			Le CPAS a-t-il fait en sorte que seuls les administrateurs agréés (gestionnaires) du réseau aient accès au système informatique ?
28	BLD DATA SEC	5.6.3	Le CPAS a-t-il sécurisé 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 ?			Le CPAS a-t-il imposé un nom d'utilisateur et un mot de passe pour chaque utilisateur ayant accès au réseau de la sécurité sociale (extranet) ?
			Ceci vérifie si l'organisation respecte les règles de gestion des accès au portail de la sécurité sociale.			
29	BLD PORTAL	5.6.1a	Le CPAS a-t-il désigné au moins un gestionnaire des accès lorsqu'il utilise les services et applications du portail de la sécurité sociale pour les besoins de ses utilisateurs ?			Le CPAS a-t-il désigné au moins un Gestionnaire Local pour les accès à la sécurité sociale ?
30	BLD PORTAL	5.6.1b	Le CPAS a-t-il recommandé à ses collaborateurs de lire et appliquer les règlements relatifs à l'utilisation des systèmes d'information des portails ?			Les collaborateurs ont-ils lu les politiques de sécurité appliquées aux accès à la sécurité sociale (exemple de politique : Politique relative à la sécurité et à la confidentialité de l'information Utilisation d'internet comme moyen d'accès au réseau de la Banque Carrefour de la Sécurité Sociale dans le cadre du traitement de données à caractère personnel par les acteurs du secteur social) ?
31	BLD PORTAL	5.6.1c	Lorsque le CPAS utilise les services et applications du portail de la sécurité sociale pour les besoins de ses utilisateurs, respecte-t-il les obligations liées à l'exercice de la fonction de gestionnaire ou de co-gestionnaire qui sont décrites dans la politique « gestion des accès aux portails » ?			Cf la politique de sécurité de la BCSS pour les gestionnaires ou co-gestionnaires du portail (https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_portal_acces_portails.pdf).

			Vérifie si l'organisation respecte les règles relatives à l'utilisation de l'IAP (Internet Access Protection).			
32		5.6.7	L'organisation du réseau primaire utilise-t-elle l'Extranet (IAP) de la sécurité sociale pour l'ensemble de ses connexions externes ou pour les connexions avec son réseau secondaire ?	NA		NA
33		5.6.7	Toute dérogation à cette mesure fait-elle l'objet d'une demande motivée introduite par l'intermédiaire du service de sécurité de la BCSS ?	NA		NA
G			**Gestion des ressources de l'entreprise lors du traitement des informations**			
			Ceci vérifie si l'organisation protège les informations de manière adéquate.			
34	BLD DATA	5.5.1a	Le CPAS dispose-t-il d'un schéma de classification interne qui est conforme à la législation spécifique en la matière et à la réglementation internationale éventuelle ?			Le CPAS a-t-il réalisé un schéma dans lequel il a identifié les données à caractère personnel qu'il traite, leur sensibilité et leur vulnérabilité et a-t-il appliqué la poilitique de Data classification (https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_data_classification_donnees.pdf) ?
35	BLD DATA	5.5.1b	L'organisation dispose-t-elle de procédures appropriées et de registres en vue de la labellisation (étiquetage) des traitements de l'ensemble des collectes de données, supports de données et systèmes d'information en cours de gestion, et ce conformément au schéma de classification interne ?			Voir le détail dans la politique de sécurité Data classification (https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_data_classification_donnees.pdf).
36	BLD DATA	5.5.1d	Les classifications de tous les systèmes critiques sont-elles définies à un niveau central par leurs propriétaires ?			Existe-t-il au CPAS un système de classification central des données très sensibles à caractère personnel centralisé ?
37	BLD DATA	5.5.1e	Les classifications de tous les systèmes critiques sont-elles contrôlées annuellement par le délégué à la protection des données (DPD) ?			

38	BLD ERASE (BLD CRYPT)	5.8.3c1	Le CPAS réalise-t-il une analyse des risques de l'utilisation du chiffrement comme mesure de base préventive contre le vol, l'abus ou la perte du support d'information ?			Le DPD a-t-il réalisé une étude de risque sur le chiffrement utilisé (risque de crackage, de durée de vie, lié au transfert de clef, etc.) ?
39	BLD ERASE	5.8.3c2	Le CPAS réalise-t-il une analyse des risques de la conformité au RGPD lorsqu'elle détruit des données à caractère personnel? Le CPAS valide-t-il les risques des méthodes utilisées durant le cycle de vie complet des données: en usage, sous forme de backup et en transit ?			Les CPAS sont essentiellement concernés par la loi organique et les contraintes des archives générales du royaume en matière de destruction des données à caractère personnel. Cette question est surtout valable pour la conservation à moyen et long terme des données par le CPAS.
40	BLD ERASE	5.8.3c3	En cas de réutilisation du support d'information, le CPAS réutilise-t-il celui-ci dans un niveau de classification des données au moins comparable (risque de protection similaire) ?			Si le CPAS a utilisé un cryptage de données pour conserver des données à caractère personnel sur un disque dur amovible (par exemple) et qu'il réutilise le support pour le stockage d'autres données, le système de cryptage utilisé pour la deuxième sauvegarde est-il au moins aussi fort que le premier ?
			Vérifie si l'organisation identifie les ressources et prend les mesures de protection adéquates.			
41	BLD APPDEV	5.5.2	Le CPAS dispose-t-il d'un inventaire du matériel informatique et des logiciels actualisé en permanence ?			
42	BLD DATA	5.5.1f	Les mesures de contrôle sont-elles conformes aux risques et et sont-elles adoptées en fonction des possibilités techniques et du coût des mesures à prendre ?			Si les risques sont élevés, les contrôles effectués le sont-ils en fonction de ces risques, de leur technicité et des coûts à réaliser ?
43	BLD PRVACY	5.15.2a	Le CPAS dresse-t-il régulièrement la carte des risques relatifs à la conformité au Règlement européen et exécute-t-il les actions devenues nécessaires suite à un risque résiduel majeur de non-conformité ?			Face au registre des traitements, le CPAS revoit-il par registre les risques liés à ceux-ci et prend-il les mesures adéquates dans le cadre du RGPD afin de supprimer ou diminuer les risques résiduels majeurs (un risque résiduel est un risque restant après avoir pris des mesures de sécurité pour le diminuer ou le supprimer) ?
44	BLD PHYS	5.8.2h	Les mesures nécessaires sont-elles prises pour que l'ensemble des données soient effacées ou rendues inaccessibles sur les supports d'enregistrement destinés à être supprimés ou réutilisés ?			Détruit-on les disques durs pour éviter que les données ne soient réutilisées ou utilise-t-on des méthodes techniques telles qu'il est certain que les données stockées sur les supports ne pourront plus jamais être lues ?

45	BLD DATA BLD DATA	5.5.5	Le CPAS a-t-il pris les mesures nécessaires pour protéger, contre les accès non autorisés, les supports en transit, notamment les backups contenant des données sensibles ?			Le CPAS crypte-t-il les données sur les supports en transit (disque dur, clef USB, smartphone avec mémoire, carte SD, ...) ?
46	BLD ERASE	5.8.3c4	Le CPAS détruit-il physiquement le support d'information lorsqu'il existe un risque résiduel non acceptable pour l'organisation que les données soient retrouvées après leur suppression ?			
H			**Médias d'enregistrement et appareils mobiles**			
			Ceci vérifie si l'organisation garantit la sécurité de l'utilisation d'appareils mobiles (smartphone, tablette, ...).			
47	BLD MOBILE	5.3.2.1c	Le CPAS impose-t-il les conditions qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils mobiles privés à des fins professionnelles ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_mobile_mobile.pdf .
48	BLD MOBILE	5.3.2.1d	Le CPAS impose-t-il les règles qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils mobiles à des fins professionnelles et à des fins privées ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_mobile_mobile.pdf .
49	BLD MOBILE	5.3.2.1i	Le CPAS dispose-t-il d'une politique pour l'usage de ses appareils mobiles à des fins privées dans le respect des règles relatives à la vie privée ?			
50	BLD MOBILE	5.3.2.1e	Le CPAS dispose-t-il d'un registre central contenant l'identification de ses appareils mobiles ?			
			Vérifie si l'organisation garantit la sécurité de l'utilisation de médias mobiles (smartphone, tablette, clé USB, disque USB, ...).			
51	BLD MOBILE	5.3.2.1a	Le CPAS prend-il les mesures adéquates afin que les données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles (tant médias qu'appareils d'enregistrement mobiles) ne soient accessibles qu'aux seules personnes autorisées ?			Ceci signifie: des contrôles d'accès ou des mesures de cryptage avec clef de chiffrement ont-ils été installés sur des médias mobiles contenant des données sensibles afin que seuls les utilisateurs agréés y aient accès ?

52	BLD MOBILE	5.3.2.1e	Le CPAS configure-t-il sur ses propres appareils mobiles la sécurité utile pour ces appareils (et les équipe-t-il des logiciels antimalware nécessaires ainsi que des logiciels permettant la suppression à distance de l'ensemble des données sur l'appareil) ?			Ceci concerne tous les appareils mobiles.
53	BLD MOBILE	5.3.2.1f	Le CPAS prévoit-il les contrôles appropriés afin de vérifier la conformité des appareils mobiles à la politique relative à la sécurité de l'information et à la vie privée (à distance au moyen d'un logiciel ou sur place au moyen d'un contrôle direct) ?			Cf la question 5.1.1 d'application ici aussi.
54	BLD MOBILE	5.3.2.1h	La possibilité de bloquer directement l'accès aux informations du CPAS (données ou applications présentes sur l'appareil mobile) et d'effacer des données existe-t-elle ?			Le CPAS a-t-il installé un système tel qu'il est possible de bloquer l'accès aux informations sur des médias mobiles ou d'effacer les informations à distance ?
I			**Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : gestion des projets ou**			
			Cette politique vérifie si l'organisation garantit les aspects relatifs à la sécurité et à la vie privée dans le cadre de la gestion des collaborateurs internes et externes participant au projet.			
55	BLD APPDEV	5.11.1	Tout projet d'acquisition, de développement ou de maintenance de systèmes a-t-il fait l'objet d'une communication constructive ente les différentes parties concernées par le projet et le délégué à la protection des données (DPD) ?			Le DPD a-t-il été informé de tout projet d'achat, de développement ou de maintenance de système informatique par les autres personnes concernées du CPAS ?
56	BLD APPDEV	5.11.7b 2	La journalisation (le « logging ») satisfait-elle, au cours d'un projet, au moins aux objectifs suivants ? • les informations permettant de déterminer qui a obtenu accès à quelles informations, à quel moment et de quelle manière ? • l'identification de la nature des informations consultées ? • l'identification précise de la personne ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
57	BLD APPDEV	5.11.7c	A-t-on tenu compte des systèmes de gestion des logs actuels lors de l'évaluation des besoins de logs dans le cadre du présent projet ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.

58	BLD APPDEV	5.11.8	Les délivrables du projet (code source, programmes, documents techniques, ...) sont-ils intégrés dans le système de gestion des sauvegardes comme imposé dans les politiques de sécurité ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
59	BLD APPDEV	5.11.11	La documentation (technique, procédures, manuels, ...) est-elle actualisée au cours de la durée de vie du projet ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
			Ceci vérifie si l'organisation garantit les aspects en matière de sécurité et de vie privée au cours du cycle de vie complet du projet.			
60	BLD HR	5.3.1.5	Le CPAS connecté au réseau de la Banque Carrefour dispose-t-il de procédures pour le développement de nouveaux systèmes ou d'évolutions importantes dans les systèmes existants, de sorte que le responsable de projet puisse tenir compte des exigences relatives à la sécurité de l'information et à la vie privée ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
61	BLD APPDEV	5.11.4	Le CPAS utilise-t-il une liste de points de contrôle pour le chef de projet de sorte que ce dernier puisse s'assurer que l'ensemble des directives relatives à la sécurité de l'information et à la vie privée sont correctement évaluées et sont, si nécessaire, mises en œuvre durant la phase de développement du	NA		Cette question est applicable aux CPAS qui font du développement informatique.
62	BLD APPDEV	5.11.14	Les aspects du « secure project lifecycle » sont-ils appliqués ? Pour plus d'informations, voir l'annexe C de la politique « Achat, conception, développement et maintenance d'applications » ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
63	BLD APPDEV	5.11.10 b	Le délégué à la protection des données (DPD) est-il informé des incidents relatifs à la sécurité de l'information et à la vie privée au cours du développement d'un projet ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
64	BLD APPDEV	5.11.6	Les dispositifs de développement, de test et/ou d'acceptation, et de production sont-ils scindés sous la supervision du chef de projet et le partage des responsabilités dans le cadre du projet qui en découle est-il réalisé ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.

J			**Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : design, mise en œuvre et tests**			
			Ceci vérifie si l'organisation respecte les conditions relatives à la protection de l'accès logique.			
65	BLD APPDEV	5.11.2c	Les conditions de protection des accès (identification, authentification, autorisation) ont-elles été définies, documentées, validées et communiquées ?			Les conditions de création des accès (nom d'utilisateur, mot de passe, eid, etc.) ont-elles été définies, documentées et validées afin que les gestionnaires soient en état de les utiliser ?
66	BLD APPDEV	5.11.2d	A-t-on évité autant que possible la gestion des accès au niveau interne dans une application ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
67	BLD APPDEV	5.11.2b	Lors du développement des protections d'accès a-t-il été tenu compte des systèmes opérationnels actuels de gestion des accès et de leur évolution ?	NA		Cette question est applicable aux CPAS qui font du développement informatique.
68	BLD APPDEV	5.11.2e	Le CPAS établit-il la relation entre le numéro de programme et l'identité de la personne physique qui envoie le message lorsqu'un programme est développé dans lequel l'institution de sécurité sociale reprend un numéro de programme dans un message qu'elle adresse à la BCSS, bien qu'une personne physique soit à l'origine de ce message ?			Cette question n'est pas applicale aux CPAS. Toutes les applications de connexion à la BCSS contiennent les informations nécessaires.
			Vérifie si l'organisation garantit les loggings en matière de sécurité et vie privée du système d'information (nouveau ou adapté).			
69	BLD APPDEV	5.9.5	La gestion des logs est-elle prévue dès le début, dans le design lors du développement ou lors de la détermination des critères d'achat de systèmes ou d'applications, afin de réaliser un « security/privacy by design » ?			Question soit pour les CPAS pratiquant le développement informatique, soit aux CPAS achetant des logiciels destinés à leur usage interne et contenant des données personnelles, soit aux deux hypothèses.
70	BLD APPDEV	5.11.2c	Les accès (identification, authentification, autorisation) font-ils l'objet d'un logging (prise de traces) ?			Le logging est un enregistrement complet de qui a fait quoi et quand.

71	BLD LOG	5.9.5	Tout accès à des données personnelles et confidentielles à caractère social ou médical fait-il l'objet d'une prise de logs, conformément à la législation et à la réglementation applicables ?			Dans ce cas-ci, cela signifie que non seulement le nom de l'utilisateur, l'heure et la date de l'accès ainsi que son action (lecture, modification, suppression) doivent être enregistrés.
72	BLD APPDEV	5.11.7b 1	Est-il précisé dans les spécifications d'un projet comment l'accès et l'utilisation des systèmes et des applications seront journalisés (« loggués »), afin de contribuer à la détection d'anomalies par rapport aux directives relatives à la sécurité de l'information et à la vie privée ?	NA		Réservé aux CPAS développant des applications.
			Ceci vérifie si l'organisation garantit la continuité, la disponibilité et la capacité nécessaires de la prestation de service.			
73	BLD APPDEV	5.11.9a	Au cours du développement du projet, les besoins relatifs à la continuité de la prestation de services sont-ils formalisés conformément aux attentes du CPAS ?			Réservé aux CPAS développant des applications. Le processus de continuité est-il appliqué lors du développement ?
74	BLD APPDEV	5.11.9f	Une analyse des risques est-elle réalisée au début du projet afin de mettre en œuvre une solution pour la disponibilité de l'application ?	NA		Réservé aux CPAS développant des applications.
75	BLD APPDEV	5.11.9b	Dans les systèmes logiciels, les points de reprise à définir afin de faire face à des problèmes opérationnels sont-ils clairement intégrés ? Les informations relatives aux points de reprise font partie du dossier d'exploitation.	NA		Réservé aux CPAS développant des applications.
76	BLD APPDEV	5.11.9c	Au cours du développement d'un projet, une attention spécifique est-elle accordée à une sauvegarde et à une restauration (« restore ») des informations ?			Réservé aux CPAS développant des applications.
77	BLD APPDEV	5.11.9d	Dans l'environnement de production, est-il tenu compte des exigences de l'organisation en ce qui concerne la redondance de l'infrastructure ?			Réservé aux CPAS développant des applications.
78	BLD APPDEV	5.11.9e	Le plan de continuité et les procédures y afférentes, en ce compris les tests de continuité, sont-ils actualisés en fonction de l'évolution du projet ?			Réservé aux CPAS développant des applications.

			Ceci vérifie si l'organisation dispose des procédures requises concernant la gestion des incidents.			
79	BLD APPDEV	5.11.10 a	Les procédures relatives à la gestion des incidents sont-elles formalisées et validées au cours du développement d'un projet ?			Réservé aux CPAS développant des applications.
			Ceci vérifie si l'organisation respecte les critères relatifs à la sécurité et à la vie privée par le nouvel environnement ou par l'environnement adapté.			
80	BLD APPDEV	5.11.5	Le CPAS s'assure-t-il lors de la mise en production du projet, que les conditions relatives à la sécurité et à la vie privée qui ont été fixées au début du projet sont effectivement mises en œuvre ? Les conditions de sécurité ont notamment trait à la confidentialité, à l'intégrité et à la disponibilité.			Réservé aux CPAS développant des applications.
81	BLD APPDEV	5.9.6	Le CPAS (participant à la transmission de données au travers de la Banque Carrefour) est-il en mesure d'assurer à son niveau la traçabilité des identifiants des employés utilisés ?			
82	BLD APPDEV	5.11.9e	Les tests visant garantir la continuité du système ICT sont-ils intégrés dans le plan de test ?			Réservé aux CPAS développant des applications.
83	BLD APPDEV	5.9.1	Le CPAS s'est-il assuré qu'aucun développement ou test n'a lieu au sein de l'environnement de production ?			Réservé aux CPAS développant des applications.
84	BLD PRIVACY		Les tests sur des données à caractère personnel sont-ils réalisés conformément au RGPD ?			Réservé aux CPAS développant des applications.

K			Achat, conception, développement et maintenance de systèmes d'information ICT (applications) : transition et support ICT			
			Cette politique vérifie si l'organisation dispose d'une procédure de « change and release management » qui a été validée au niveau des risques en matière de sécurité et de vie privée.			
85	BLD APPDEV	5.9.2	Le CPAS dispose-t-il de procédures pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes ?			Réservé aux CPAS développant des applications.
86	BLD APPDEV	5.9.2	Le CPAS a-t-il pris les mesures nécessaires afin d'éviter qu'une seule et même personne n'assure le contrôle du processus de ´mise en production (release management)` ?			Réservé aux CPAS développant des applications.
87	BLD APPDEV	5.11.12	Tous les actifs, en ce compris les systèmes acquis ou développés, sont-ils ajoutés au système de gestion des moyens opérationnels (inventaire des supports de données et systèmes d'information) ?			Réservé aux CPAS développant des applications.
			Ceci vérifie si la plateforme adaptée dispose d'une gestion des logs garantissant les conditions (légales) en matière de sécurité et de vie privée.			
88	BLD LOG	5.9.5	Le CPAS dispose-t-il d'une procédure validée, actuelle et formelle de gestion des traces, et ce pour les « privacy, sécurité, techniques et business logs » ? (planifier, exécuter, contrôler et rectifier)			Cf la politique de sécurité suivante (chapitre C) : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_log_gestion_logs.pdf
89	BLD LOG		Les « privacy logs » donnent-ils au moins une réponse aux questions suivantes : quoi, quand, quelle organisation, comment, concernant qui, action réussie ou non ?			Idem
90	BLD LOG	5.11.7e	Les « privacy logs » sont-ils conservés pendant 10 ans au moins ?			
91	BLD LOG	5.9.5	Les fichiers logs sont-ils conservés pendant une période convenue, pour les investigations et contrôles futurs et ce en conformité avec la législation et la réglementation ?			Ne pas oublier de prendre en compte les durées de conservation exigées par les archivistes du royaume (en dehors des 10 ans imposés pour les logs de la sécurité sociale).

92	BLD LOG	5.9.5	Existe-t-il une procédure organisée au sein du CPAS pour les consultations des fichiers de logs techniques, entreprise de sécurité et de vie privée, avec un historique des requêtes approuvées/exécutées ou rejetées ?			
93	BLD LOG	5.9.5	Des fichiers de logs spécifiques sont-ils créés pour les logs techniques, de business, de sécurité et relatifs à la vie privée ?	NA		Cf la politique de sécurité suivante (chapitre C) : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_log_gestion_logs.pdf
94	BLD LOG	5.9.5	Le résultat de la gestion des logs est-il analysé, rapporté et évalué à des intervalles réguliers ?			
95	BLD LOG	5.9.5	La procédure de gestion des logs a-t-elle été communiquée aux collaborateurs concernés (notamment développeurs et designers ICT, collaborateurs en support ICT, responsables business, service juridique) ?			Attention, cette procédure doit prévoir également les modalités de contrôle, modalités agréées par le Conseil de l'Action Sociale et intégrées au règlement du personnel.
96	BLD LOG	5.9.5	Les horloges internes de l'ensemble des systèmes d'information de l'organisation sont-elles synchronisées avec une source temporelle précise et déterminée, de sorte qu'une analyse fiable des fichiers logs sur les différents systèmes d'information soit toujours possible ?			Toutes les horloges des serveurs sont-elles à la même heure ?
97	BLD LOG	5.9.5	Les fichiers logs sont-ils protégés contre toute consultation par des personnes non autorisées, toute modification ou toute suppression ?	NA		Il appartient au DPD de s'assurer lors de l'achat de chaque système - application que les fichiers logs sont protégés contre toute consultation non autorisée.
98	BLD LOG	5.9.5	Les outils nécessaires sont-ils disponibles ou développés que sorte que les données de logs puissent être analysées par les personnes autorisées ?			Il s'agit le plus souvent de politique de contrôle des logs à mettre en place et à faire valider par le Conseil de l'Action Sociale.
99	BLD LOG	5.9.5	Les logs techniques et plus précisément l'utilisation du système ICT font-ils l'objet de prises de traces automatiques ?	NA		Réservés aux informaticiens ou aux sociétés ayant vendu leur application.

100	BLD LOG	5.9.5	Les logs techniques et plus précisément l'utilisation du système ICT sont-ils enregistrés manuellement dans un fichier journal ?	NA		
L			**Garantir la continuité et la disponibilité de systèmes d'information de l'institution et ICT**			
			Cette politique vérifie si le CPAS dispose d'une gestion de la continuité (planifier, exécuter, contrôler et rectifier) pour, au minimum, les processus critiques et les systèmes d'information essentiels.			
101	BLD BCM	5.14.1a	Existe-t-il un plan de continuité pour l'ensemble des processus critiques et systèmes d'information essentiels de l'organisation ?			Plan de continuité = plan catastrophe.
102	BLD BCM	5.14.1b	La sécurité de l'information et la vie privée font-elles partie intégrante de la gestion de la continuité ?			
103	BLD BCM	5.14.1c	Le CPAS a-t-il mis au point un plan de continuité contenant les informations minimales telles que décrites dans la politique « gestion de la continuité » ?			
104	BLD BCM	5.14.1e	Le plan de continuité est-il régulièrement testé et adapté et fait-il l'objet de la communication utile à la direction en vue de sa validation et de son approbation ?			
			Ceci vérifie si le CPAS dispose d'un système approprié de sauvegarde et de restauration pour ses systèmes d'information.			
105	BLD (DATA SEC) (BLD	5.9.4	L'organisation a-t-elle défini la politique et la stratégie organisant la mise en œuvre d'un système de sauvegarde en phase avec la gestion de la continuité ?			
106	BLD (DATA SEC)	5.9.4	Le CPAS a-t-il régulièrement contrôlé les sauvegardes réalisées dans ce cadre ?			

			Ceci vérifie si le CPAS applique les mesures assurant la disponibilité de l'alimentation et la protection physique des appareils, afin de garantir la continuité.			
107	BLD PHYS (BLD BCM)	5.8.2b	Le CPAS dispose-t-il d'une alimentation (électrique) alternative afin de garantir la prestation de services attendue ?			
108	BLD PHYS (BLD BCM)	5.8.2c	Les appareils critiques sont-ils protégés contre une panne de courant ou d'autres dysfonctionnements par une rupture de l'alimentation (p.ex. eau, chauffage, refroidissement) ?			
109	BLD PHYS	5.8.2a	Les appareils critiques sont-ils installés et protégés de manière à réduire les risques d'endommagement et de dysfonctionnement de l'extérieur ?			
M			**Protection de la communication implémentée au moyen des ICT**			
			Ceci vérifie si le CPAS dispose de mesures de sécurité pour l'usage des réseaux sans fil pour lesquels elle est responsable.			
110	BLD WIREL	5.10.1a	Le CPAS dispose-t-il, pour l'ensemble des réseaux sans fil qu'il a sous sa gestion et à tous les endroits, d'un processus permettant d'obtenir un aperçu de l'ensemble des réseaux sans fil existants et autorisés, des protocoles de sécurité utilisés par ces réseaux, et de l'ensemble des mesures de sécurité qui y sont associées ?	NA		
111	BLD WIREL	5.10.1b	Le CPAS respecte-t-il les directives qui sont décrites dans l'annexe C de la politique « réseaux sans fil sécurisés » ?	NA		
			Ceci vérifie si le CPAS dispose de mesures de sécurité pour l'usage des réseaux.			
112	BLD WIREL	5.10.2	Le CPAS vérifie-t-il que les réseaux sont gérés et contrôlés de manière adéquate afin de les protéger contre les menaces ?			Cette question implique la présence d'antivirus, de parefeu, de systèmes de détection d'instruction et de systèmes de détection de cryptolockers (sandboxing par exemple).

113	BLD WIREL	5.10.3	Le CPAS a-t-il mis en place les mesures techniques nécessaires, suffisantes, efficientes et adéquates en vue de garantir la plus haute disponibilité de connexion avec le réseau de la Banque Carrefour et ce afin d'assurer une accessibilité maximale aux données tant mises à disposition que consultées ?			Cette question vise à savoir si le CPAS peut se connecter à un autre accès internet en cas de panne de sa connexion habituelle, en disposant par exemple d'une autre connexion physique ou d'un modem avec un interrupteur 4G permettant de travailler uniquement en 4G.
114	BLD WIREL	5.10.4	Le CPAS dispose-t-il d'une cartographie actualisée des flux techniques (au niveau du réseau sont nécessaires à la gestion des firewalls dans les différentes zones de l'Extranet) mis en œuvre au travers de l'Extranet (IAP) de la sécurité sociale ?			Un diagramme décrivant l'architecture du réseau du CPAS avec ses appareillages et ses systèmes de sécurité existe-t-il ?
			Ceci vérifie si l'organisation dispose de mesures de sécurité pour l'utilisation du « Courriel, de la communication en ligne et d'internet » par les collaborateurs internes et externes (temporaires).			
115	BLD ONLINE	5.5.4a	Le CPAS a-t-il intégré dans sa politique relative à la sécurité de l'information et à la vie privée les règles qui sont spécifiées à l'annexe C de la politique « E-mail, communication en ligne et utilisation d'internet » ?			Cf les politiques de sécurité de l'email et de l'internet disponible sur le site de la BCSS : https://www.ksz-bcss.fgov.be/fr/protection-des-donnees/politique-de-securite-de-linformation .
116	BLD ONLINE	5.5.4b	Le CPAS exerce-t-il en permanence un contrôle sur l'e-mail, la communication en ligne et l'utilisation d'internet dans le cadre des objectifs suivants : • la protection de la réputation et des intérêts de l'organisation; • la prévention de faits illicites ou de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui; • la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'organisation, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'organisation; • le respect des principes clés ?			Attention, ce contrôle doit s'effectuer dans un cadre légal avec une politique de sécurité agrée par le Conseil de l'Action Sociale et dans le règlement du personnel pour prévoir les sanctions.

N			Télétravail et accès en ligne en dehors de l'organisation			
			Cette politique vérifie si le CPAS dispose de mesures adéquates afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors du CPAS aux données sensibles, confidentielles et professionnelles de l'organisation.			
117	BLD TELE	5.3.2.2a	Le CPAS a-t-il pris les mesures adéquates, en fonction du moyen d'accès (p.ex. Internet, ligne louée, réseau privé, réseau sans fil), afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de Le CPAS aux données sensibles, confidentielles et professionnelles de l'organisation ?	NA		
			Vérifie si le CPAS dispose de règles de bonne conduite précises dans le cadre du télétravail.			
118	BLD TELE	5.3.2.2b	L'organisation a-t-elle clairement mis au point des règles de bonne conduite ainsi qu'une mise en œuvre appropriée du télétravail, les a-t-elle validées, communiquées et tenues à jour? L'organisation doit aussi préciser quels systèmes peuvent et quels systèmes ne peuvent pas être consultés au départ du lieu de travail à domicile ou d'autres appareils ?	NA		
119	BLD TELE	5.3.2.2c	L'organisation a-t-elle organisé les dispositifs de télétravail de l'organisation de la sorte que sur le lieu du télétravail (à domicile, dans un bureau satellite ou à un autre endroit) aucune information relative à l'organisation ne soit enregistrée sur des appareils externes sans chiffrement et qu'aucune menace potentielle ne puisse atteindre l'infrastructure IT de l'institution au départ du lieu de télétravail ?	NA		

0			**Mise en place de mesures de chiffrement**			
			Vérifie si l'organisation dispose d'une politique formelle en vue de l'utilisation de mesures cryptographiques.			
120	BLD CRYPT	5.7.1a	Le responsable de la sécurité ICT définit-il les mesures cryptographiques qu'il y a lieu d'appliquer dans les différents cas, compte tenu des bonnes pratiques en la matière et d'une analyse des risques ?			Cf la politique de chiffrement : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
121	BLD ERASE	5.7.1b	L'organisation réalise-t-elle une analyse des risques de l'utilisation du chiffrement comme mesure de base préventive contre le vol, l'abus ou la perte du support d'information ?			Cf la politique de chiffrement : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
122	BLD CRYPT	5.7.1c	L'organisation tient-elle à jour une liste des endroits où des mesures cryptographiques sont appliquées, des mesures cryptographiques qui sont appliquées et de la personne qui est responsable de ces mesures ?			Cf la politique de chiffrement : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
123	BLD CRYPT	5.7.1d	L'application et l'adéquation de mesures et solutions cryptographiques sont-elles évaluées périodiquement ?			Cf la politique de chiffrement : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
124	BLD CRYPT	5.7.1e	Les données chiffrées de tiers qui entrent dans le réseau de l'organisation sont-elles d'abord déchiffrées et scannées pour détecter la présence de virus et autres malware ?			Cf la politique de chiffrement : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
			Vérifie si le CPAS dispose d'une politique formelle pour l'utilisation, la protection et la durée de vie des clés cryptographiques pour le cycle de vie complet.			
125	BLD CRYPT	5.7.1f	Des processus et procédures spécifiques relatifs à la gestion des clés ont-ils été rédigés, validés et communiqués à l'ensemble des acteurs concernés ? Ces processus et procédures font-ils aussi l'objet d'une maintenance régulière ? Il s'agit de processus relatifs à la demande/génération de clés; à l'enregistrement de clés (privées); au transport de clés (privées); à l'utilisation de clés; au remplacement et à la destruction de clés; à l'archivage de clés; à la résolution de clés compromises.			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf

126	BLD CRYPT	5.7.1g	Un collaborateur interne est-il responsable pour toute clé ? Une liste de l'ensemble des responsables des clés est-elle tenue à jour ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
127	BLD CRYPT	5.7.1h	Existe-t-il des mesures permettant de détecter des tentatives non autorisées de diffusion, de déchiffrement, d'accès, d'usage, de modification ou de remplacement de clés ou de données chiffrées ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
128	BLD CRYPT	5.7.1i	L'accès aux clés privées et leur utilisation fait-il l'objet de prise de traces conformément aux procédures de gestion des logs ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
129	BLD CRYPT	5.7.1j	Les contrats avec les fournisseurs de services ou produits cryptographiques contiennent-ils des directives de l'organisation en rapport avec la gestion de clés ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_crypt_chiffrement.pdf
P			**Relations avec des fournisseurs et travaux avec une tierce partie**			
			Cette politique vérifie si des garanties suffisantes ont été définies de sorte que le traitement par la tierce partie et/ou le fournisseur satisfait aux conditions légales et aux conditions de sécurité.			
130	BLD OUTS	5.12.1a	Les obligations en matière de traitement de données à caractère personnel sont-elles fixées dans un contrat, conformément au RGPD, lorsque le CPAS sous-traite du travail à un fournisseur (sous-traitant) ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf .
131	BLD OUTS	5.12.1b	Les conditions relatives à la sécurité de l'information et à la vie privée font-elles l'objet d'un accord avec les tiers et sont-elles documentées afin de réduire les risques relatifs à l'accès des tiers aux informations ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf .
132	BLD OUTS	5.11.3	Lors de la sous-traitance à des tiers, les conditions relatives à la sécurité et à la vie privée sont-elles fixées contractuellement et des clauses de confidentialité et de continuité sont-elles prévues ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf .

133	BLD OUTS	5.12.1c	Les fournisseurs (auxquels le travail est sous-traité et qui lisent, traitent, enregistrent, communiquent des informations de l'organisation ou qui fournissent des éléments d'infrastructure ICT) ont-ils répondu à toutes les questions du questionnaire « normes minimales fournisseurs » ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf .
134	BLD OUTS	5.12.1d	Les contrats conclus avec les tiers (fournisseurs) comprennent-ils toutes les conditions permettant de traiter les risques liés à la sécurité de l'information et à la vie privée qui sont afférents aux services ICT ?			Cf la politique de sécurité https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf .
			Ceci vérifie si la prestation de service par le fournisseur ou la tierce partie fait régulièrement l'objet d'une évaluation.			
135	BLD OUTS	5.12.1e	Le CPAS effectue-t-il régulièrement un contrôle de la prestation de service de tiers et évalue-t-il ou audite-t-il cette prestation de service ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf
136	BLD OUTS	5.12.1f	Les adaptations de la prestation de service sont-elles gérées par des tiers ? Par adaptations, on entend notamment l'actualisation et l'amélioration des politiques, procédures et mesures relatives à la sécurité de l'information et à la vie privée existantes.			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf
			Ceci vérifie si le CPAS fixe les mesures appropriées de suppression de données dans un contrat avec des tiers.			
137	BLD ERASE	5.8.3e1	Le CPAS fixe-t-il les mesures adéquates de suppression de données dans un contrat lorsqu'il procède à la lecture des supports d'information ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf
138	BLD ERASE	5.8.3e2	Le CPAS fixe-t-il les mesures adéquates de suppression de données dans un contrat lorsqu'il utilise (provisoirement) des supports de données lors d'un disaster recovery ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf
139	BLD ERASE	5.8.3e3	Le CPAS fixe-t-il les mesures adéquates de suppression de données dans un contrat dans le cadre du cloud computing ?			https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_outs_sous_traiter.pdf

Q			**Systèmes d'information Cloud ICT**			
			Ceci vérifie si le CPAS qui utilise une solution cloud respecte les prescriptions.			
140	BLD CLOUD	5.12.2a	Lorsque le CPAS fait appel aux services d'un cloud, le fait-il en conformité avec les dispositions décrites au point 2.1 de la politique « Cloud computing » ?			Cf la politique suivante : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_cloud_cloud.pdf
141	BLD CLOUD	5.12.2b	Lorsque le CPAS souhaite traiter des données sensibles, confidentielles ou professionnelles dans un cloud, satisfait-il aux garanties contractuelles minimales et aux directives telles que décrites au point 2.2, 2.3 et 2.4 de la politique « Cloud computing » ?			Cf la politique suivante : https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_cloud_cloud.pdf
R			**Respect**			
			Ceci vérifie si le CPAS respecte les obligations (légales) et directives dans le domaine de la sécurité et de la vie privée.			
142	BLD APPDEV	5.11.13	La collaboration appropriée à des fins d'audit interne et externe de la sécurité et de la vie privée dans le processus « Achat, conception, développement et maintenance de systèmes d'information ICT » est-elle apportée sous la forme de mise à la disposition du personnel, de la documentation, de la gestion des traces et des autres informations qui sont raisonnablement disponibles ?			Le CPAS met-il du personnel à disposition des auditeurs si cela s'avère nécessaire en aidant les auditeurs, en mettant à leur disposition de la documentation, des logs et toute information nécessaire ?
143	BLD COMPLY	5.15.1e	Les domaines décrits dans l'annexe C de la directive « respect » sont-ils vérifiés lors de l'élaboration des différents audits ?			On entend par respect le respect des points suivants : 1. périodiquement mener un audit de conformité concernant l'état de la sécurité et de la confidentialité de l'information comme décrit dans les politiques; 2. éviter la violation de toute disposition légalerelative à la sécurité et à la confidentialité de l'information; 3. s'assurer que la politique de sécurité et de confidentialité de l'information est mise en oeuvre conformément aux attentes de la direction; 4. prévoir une procédure disciplinaire formelle pour les travailleurs qui violent la politique de sécurité et de confidentialité de l'information.
144	BLD COMPLY	5.15.1a	Le CPAS réalise-t-il périodiquement un audit de conformité de la situation relative à la sécurité de l'information et à la vie privée telle que décrite dans les politiques de sécurité ?			

145	BLD KSZ	5.6.4	Le CPAS dispose-t-il des autorisations nécessaires du comité de sécurité de l'information compétent pour l'accès aux données (sociales) à caractère personnel gérées par une autre organisation ?	NA		Oui, tous les accès ont été donnés par la Commission de la vie privée.
146	BLD PRVACY	5.15.2b	Le CPAS dispose-t-il du 'registre des activités de traitement` nécessaire et à jour en tant que sous-traitant ou responsable du traitement ?			
S			**Gestion des incidents**			
			Ceci vérifie si le CPAS dispose d'un processus de gestion des incidents relatifs à la sécurité et à la vie privée et à la suppression des vulnérabilités.			
147	BLD INCID	5.13.1g	La « directive relative à la gestion des incidents » est-elle appliquée telle que décrite dans l'annexe C de la politique « Gestion des incidents » ?			Cf la Directive https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_incid_incident.pdf
148	BLD INCID	5.13.1f	Tout incident relatif à la sécurité de l'information et à la vie privée est-il évalué de manière formelle, de sorte que les procédures et mesures de contrôle puissent être améliorées? Les leçons tirées d'un incident sont-elles communiquées à la direction de l'organisation, en vue de la validation et de l'approbation d'actions futures ?			En cas d'incident, un rapport officiel est-il rédigé pour pouvoir étudier les effets, leur fréquence et les mesures correctrices apportées ? La Direction en est-elle informée ?
149	BLD INCID	5.13.1e	En cas d'incidents relatifs à la sécurité de l'information ou à la vie privée, les preuves sont-elles collectées conformément aux prescriptions réglementaires et légales (notamment la réglementation RGPD) ?			Cf les preuves à récolter en cas d'incidents (RGPD).
150	BLD INCID	5.13.1c	Les événements et failles relatifs à la sécurité de l'information ou à la vie privée en rapport avec les informations et les systèmes d'information sont-ils communiqués, de sorte que le CPAS puisse prendre, en temps utile, des mesures correctrices adéquates ?			Existe-t-il un système interne de communication en cas d'incident afin de pouvoir prendre les mesures de sécurité correctives le plus rapidement possible ?
151	BLD INCID	5.9.7	Le CPAS a-t-il installé un système et des procédures formelles et actualisées permettant la détection, le suivi et la réparation d'infractions au niveau de la sécurité proportionnellement au risque technique / opérationnel ?			Le CPAS sait-il comment réagir en fonction de la gravité de l'incident et a-t-il mis au point une procédure adéquate, quitte à faire appel à une société extérieure ?

152	BLD INCID	5.13.1a	Le CPAS dispose-t-il de procédures pour la détermination et la gestion d'incidents relatifs à la sécurité de l'information ou à la vie privée et des responsabilités s'y rapportant et a-t-il communiqué ces procédures à ses collaborateurs ?			
153	BLD INCID	5.13.1d	Les incidents relatifs à la sécurité de l'information et à la vie privée sont-ils rapportés, dans les meilleurs délais, à l'intervention du supérieur hiérarchique, du helpdesk, du délégué à la protection des données (DPD) et ce conformément aux procédures de gestion des incidents ?			
154	BLD (DATA SEC)	5.9.3	Le CPAS dispose-t-il de systèmes actualisés pour se protéger (prévention, détection et rétablissement) contre des codes nocifs ?			Cette question implique la présence d'antivirus, de parefeu, de systèmes de détection d'instruction et de systèmes de détection de cryptolockers (sandboxing par exemple).

Veuillez renvoyer le questionnaire complété digitale pour **le 30 septembre 2019** au plus tard au Service Sécurité de l'information de la Banque Carrefour de la sécurité sociale (security@ksz-bcss.fgov.be) .

Modalité à respecter par les institutions du réseau secondaire :

Les institutions du réseau secondaire remettent le questionnaire complété à l'institution de gestion qui transmet les listes reçues au Service Sécurité de l'information de la Banque Carrefour pour la date mentionnée ci-dessus.

Date et signature du délégué à la protection des données (Le CPASDPD) (facultatif)	*[Date]*	*[Signature']* X Name
Date et signature de la personne chargée de la gestion journalière de l'institution **(obligatoire)**	*[Date]*	*[Signature']* X

INTÉGRATION SOCIALE

QUESTIONS ?