Normes minimales sécurité de l'information et vie privée

(MNM)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie relative à la sécurité de l'information et à la vie privée au sein de la sécurité sociale. Le présent document est destiné aux responsables, aux sous-traitants de données, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

L'organisation de la politique relative à la sécurité de l'information et à la vie privée au sein du réseau de la Banque Carrefour de la sécurité sociale est basée sur l'application obligatoire des normes minimales relatives à la sécurité de l'information et à la vie privée par ses partenaires, tel que prévu à l'arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale*.

Les normes minimales relatives à la sécurité de l'information et à la vie privée créent les conditions nécessaires pour une exécution fiable du traitement de l'information dans le chef des institutions publiques de sécurité sociale (IPSS) intégrées au réseau de la Banque Carrefour de la sécurité sociale.

Il est essentiel pour les partenaires au sein de la sécurité sociale de connaître ces normes minimales relatives à la sécurité de l'information et à la vie privée, de les valider, de les communiquer et de les intégrer.

Le présent document décrit les normes minimales de la sécurité de l'information et de la vie privée.

2. Champ d'application des normes minimales

L'application des normes minimales relatives à la sécurité de l'information et à la vie privée est obligatoire pour les institutions de sécurité sociale en vertu de l'article 2, alinéa 1er, 2° de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale (BCSS). De plus, l'application des normes minimales relatives à la sécurité de l'information et à la vie privée concerne aussi toutes les instances qui font partie du réseau de la sécurité sociale en vertu de l'article 18 de cette loi. Enfin, le Comité sectoriel de la sécurité sociale et de la santé peut aussi imposer le respect des normes minimales relatives à la sécurité de l'information et à la vie privée à des instances autres que celles précitées.

Les normes minimales décrites dans le présent document doivent obligatoirement être respectées par les organisations si elles souhaitent accéder et maintenir l'accès au réseau de la Banque Carrefour de la sécurité sociale. Ces normes minimales ont donc une valeur contraignante.

Certaines organisations occupent plusieurs bâtiments ou disposent de (petits) bureaux régionaux. Les normes minimales relatives à la sécurité de l'information et à la vie privée doivent aussi y être respectées.

En outre, les normes ne s'appliquent en principe qu'au traitement de données sociales à caractère personnel. Les normes minimales relatives à la sécurité de l'information et à la vie privée doivent toutefois également être appliquées dans le cadre de la délibération n° 21/2004 du 12 juillet 2004, par laquelle certaines institutions de sécurité sociale ont été autorisées par la Commission de la protection de la vie privée à obtenir, sous certaines conditions, accès au Registre national et à utiliser le numéro d'identification du Registre national pour la réalisation de leurs tâches en matière de gestion du personnel.

Par ailleurs, il est de bon usage que ces normes s'appliquent également à la sécurité de l'information et à la vie privée au sens large du terme, comme prévu à l'arrêté royal du 17 mars 2013 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 et comme repris dans l'arrêté royal du 12 août 1993 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 ».

Enfin, le Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel du 27 avril 2016[1] a un impact important sur la sécurité de l'information et la vie privée de l'ensemble des institutions de sécurité sociale.

3. Objectifs

Ces normes minimales relatives à la sécurité de l'information et à la vie privée visent à:

A. à garantir le respect des obligations légales et réglementaires applicables;

B. à maintenir la confiance des citoyens dans les échanges de données avec les pouvoirs publics;

C. assurer, d'une manière coordonnée, un niveau approprié en ce qui concerne la sécurité de l'information et la vie privée;

D. à obtenir ou conserver l'autorisation d'échanger des données au sein du réseau de la Banque Carrefour de la sécurité sociale (BCSS).

4. Quoi et pourquoi?

4.1. La sécurité de l'information, c'est quoi ?

Les informations constituent un actif essentiel nécessitant une protection adéquate. Dans le monde actuel en pleine évolution, les informations n'ont jamais été autant exposées à toute sorte de menaces et de vulnérabilités.

Les informations, sous quelque forme que ce soit (écrite, orale, imprimée, envoi par la poste ou par la voie électronique), doivent, à tout moment, être protégées de manière adéquate contre les vulnérabilités et menaces internes et externes. La responsabilité d'assurer la continuité du traitement des données et de gérer la confidentialité et l'intégrité des informations incombe à chaque direction et à chaque sous-traitant de données.

Chaque organisation poursuit la sécurité de l'information au moyen de mesures de contrôle effectives et efficaces. Ces mesures de contrôle doivent être gérées de manière dynamique et optimalisées de manière continue là où cela s'avère nécessaire, afin de réaliser de la sorte l'objectif de l'organisation. Chaque organisation intègre la sécurité de l'information autant que possible directement dans l'ensemble de ses processus.

4.2. La vie privée, c'est quoi ?

Tout individu a droit à la protection de ses données à caractère personnel: « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[2].

Par ailleurs, tout individu a droit à la protection du traitement de ses données à caractère personnel: « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Chaque organisation poursuit la protection de la vie privée au moyen de mesures de contrôle effectives et efficaces. Ces mesures de contrôle doivent être gérées de manière dynamique et optimalisées de manière continue là où cela

[1] EU GDPR http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

[2] Définition de données à caractère personnel telle que contenue dans le EU GDPR http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

s'avère nécessaire, afin de réaliser de la sorte l'objectif de l'organisation. Chaque organisation intègre la protection de la vie privée autant que possible directement dans l'ensemble de ses processus.

4.3 Pourquoi la sécurité de l'information et la vie privée sont-elles essentielles?

Les informations et les processus, systèmes et réseaux y afférents constituent des actifs importants pour une organisation. La définition, la mise en œuvre, la maintenance et l'amélioration de la sécurité de l'information et de la vie privée sont essentielles afin de garder intact la confiance des citoyens, de (continuer à) respecter les obligations légales et de préserver la réputation de l'organisation.

Les mesures technologiques ne couvrent pas tout et doivent toujours être complétées par les éléments organisationnels, de procédure et de communication appropriés qui sont basés sur une évaluation des risques ou sur des obligations réglementaires ou légales.

La gestion de la sécurité de l'information et de la vie privée requiert la participation active de tous les collaborateurs, citoyens, organisations, fournisseurs et autres parties externes. En effet, une organisation, en ce compris les informations et systèmes d'information, est confrontée à des menaces et problèmes divers. Ces menaces et problèmes sont de plus en plus fréquents. L'attaque de systèmes informatiques est simple à organiser à petit prix. Les attaques sont de plus en plus sophistiquées. Les problèmes se complexifient. Les mesures de contrôle appropriées permettant de les maîtriser (prévenir et guérir) requièrent de la compréhension, un planning et des moyens suffisants.

5. Normes minimales

Toute organisation souscrit les normes minimales suivantes relatives à la sécurité de l'information et à la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation:

5.1. Principes clés

	Objet	Norme minimale
5.1.1	Principes clés	Toute organisation doit intégrer les principes clés dans sa politique de sécurité de l'information.

5.2. Politique de sécurité de l'information

	Sujet	Norme minimale
5.2.1	Information Security Policy[3].	Toute organisation doit disposer d'une politique de sécurité de l'information formelle et actualisée, approuvée par le responsable de la gestion journalière

3 La présente Information Security Policy (ISP) s'inscrit dans le cadre d'un système de gestion de la sécurité de l'information : le groupe de travail "Sécurité de l'information" a pris l'initiative de développer un ISMS (Information security Management System), qui s'inspire de la norme ISO 27001, afin de répondre à un besoin des institutions du réseau de disposer d'une politique de sécurité structurée et commune. L'ISMS est un système intégré qui doit permettre une protection optimale des informations. Les mesures concrètes pour parvenir à une sécurité de l'information optimale sont des « mesures de politique » ou des « contrôles ». L'ISMS est considéré comme la **méthodologie commune** à appliquer par les institutions du réseau pour parvenir à une sécurité maximale de l'information. **Il appartient aux institutions de sécurité sociale d'adapter l'ISMS à leur situation spécifique et à l'importance des moyens de fonctionnement à protéger.** En ce qui concerne sa mise en œuvre, le conseiller en sécurité de l'information de chaque institution doit obtenir une décision de sa hiérarchie. L'ISMS commun a été approuvé en ces termes par le Comité général de coordination : « Il s'agit d'un document de base à utiliser en interne par les institutions. L'ISMS, qui est basé sur la norme ISO 27002, contient les lignes directrices à respecter. Une concertation permanente doit être organisée entre le conseiller en sécurité et le personnel dirigeant. »).

		(ou équivalent).
5.2.2	Evaluation des risques	Toute organisation doit : a. pour tout processus et pour tout projet réaliser une évaluation des risques au niveau de la sécurité de l'information et de la vie privée, la valider, la communiquer et la maintenir b. communiquer toutes les évaluations de risques à risque résiduel majeur à la direction afin de les examiner et de prendre une décision à ce sujet: les traiter ou les accepter. c. appliquer la directive relative à l'évaluation des risques telle que mentionnée dans l'annexe C de la politique « évaluation des risques ».

5.3. Organisation de la sécurité de l'information

5.3.1. Organisation interne

	Objet	**Norme minimale**
5.3.1.1	Aspects liés aux personnes	Toute organisation doit préalablement au contrat de travail • vérifier le milieu familial et socioculturel des candidats aux fonctions qui impliquent un risque majeur pour la sécurité de l'information; cette vérification doit être réalisée conformément aux lois et prescriptions pertinentes et doit être proportionnelle aux exigences, à la classification des informations auxquelles l'accès est accordé et aux risques estimés. • Dans le cadre de leur obligation contractuelle, le personnel auquel il est fait appel et les collaborateurs externes doivent accepter les conditions générales et doivent signer leur contrat de travail, qui fixe leurs responsabilités et celles de l'organisation par rapport à la sécurité de l'information et à la vie privée. Pendant le contrat de travail: • La direction doit exiger des travailleurs, du personnel auquel il est fait appel et des utilisateurs externes qu'ils appliquent la sécurité de l'information et la vie privée, conformément aux normes minimales et aux procédures de l'organisation. • Tous les travailleurs de l'organisation et, si applicable, le personnel auquel il est fait appel et les utilisateurs externes doivent recevoir un entraînement approprié et suivre régulièrement une formation continue relative aux normes minimales et aux procédures de l'organisation, pour autant que cela soit pertinent pour leur rôle ou fonction. • actualiser régulièrement la vérification du milieu familial et socioculturel des candidats aux fonctions qui impliquent un risque majeur pour la sécurité de l'information et la vie privée, conformément aux lois et prescriptions pertinentes. Cette vérification doit être proportionnelle aux exigences, à la classification des informations auxquelles l'accès est accordé et aux risques estimés. • Il y a lieu de prévoir une procédure disciplinaire formelle pour les collaborateurs ayant commis une infraction à la sécurité de l'information et à la vie privée, et ce conformément aux sanctions en cas de non-

	Objet	Norme minimale
		respect telles que prévues dans la législation Cessation ou modification du contrat de travail: • Les responsabilités et obligations relatives à la sécurité de l'information et à la vie privée qui restent valables après la cessation ou la modification du contrat de travail doivent être clairement définies, communiquées au collaborateur, au personnel auquel il est fait appel et aux collaborateurs externes et doivent être rendues obligatoires.
5.3.1.2	Organisation de la sécurité de l'information	Toute organisation doit : a. instaurer un service de sécurité de l'information placé sous la direction d'un conseiller en sécurité de l'information ou confier cette tâche à un service de sécurité de l'information spécialisé agréé. b. communiquer l'identité de son conseiller en sécurité et de ses adjoints éventuels au comité sectoriel de la sécurité sociale et de la santé. Pour les organisations du réseau secondaire, l'identité doit être communiquée à l'institution responsable de ce réseau. c. disposer d'un plan de sécurité approuvé par le responsable de la gestion journalière (ou équivalent) de l'organisation concernée. d. disposer des crédits de fonctionnement nécessaires, approuvés par le responsable de la gestion journalière de l'organisation concernée (ou équivalent), en vue de l'exécution de son plan de sécurité et de l'exécution par le service de sécurité des tâches qui lui ont été confiées. e. communiquer à la BCSS le nombre d'heures qu'elle a officiellement accordé à son conseiller en sécurité et à ses adjoints éventuels pour l'exécution de leurs tâches. f. organiser une communication périodique d'informations au conseiller en sécurité de sorte que celui-ci dispose des données nécessaires pour l'exécution de sa mission de sécurité ainsi que pour l'organisation de la concertation entre les différentes parties concernées[4] afin d'associer davantage le conseiller en sécurité aux travaux de l'organisation.
5.3.1.3	Plateforme de décision[5]	Toute organisation doit disposer d'une plateforme de décision pour valider et approuver les mesures relatives à la sécurité de l'information et à la vie privée.
5.3.1.4	Réseau secondaire	Toute organisation gérant un réseau secondaire doit échanger, au moins une fois par semestre, des informations pertinentes avec son réseau secondaire, en organisant une réunion du sous-groupe de travail « Sécurité de l'information » pour les organisations qui font partie de son réseau.
5.3.1.5	Sécurité de l'information dans le cadre de projets	Toute organisation doit disposer de procédures pour le développement de nouveaux systèmes ou d'évolutions majeures dans les systèmes existants, de sorte que le responsable de projet tienne compte des exigences relatives à la sécurité de l'information et à la vie privée décrites dans le présent document.

5.3.2. Appareils mobiles et télétravail

4 Les parties visées dans cette norme sont principalement les membres du service informatique (développement et production), le conseiller en prévention, le conseiller en sécurité et les services de gestion des données.

5 La plateforme de décision oriente la politique de sécurité : la révision de la politique, l'adaptation des mesures de sécurité, l'élaboration de plans de sécurité, la détermination des responsabilités et la surveillance de l'évolution des menaces et des incidents.

	Objet	Norme minimale
5.3.2.1	Utilisation sécurisée d'appareils mobiles	Toute organisation doit a. prendre les mesures adéquates afin que les données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles ne soient accessibles qu'aux seules personnes autorisées. b. prendre les mesures adéquates, en fonction du moyen d'accès[6], afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de l'organisation aux données sensibles, confidentielles et professionnelles de l'organisation. c. imposer les conditions qui sont détaillées dans la politique « appareils mobiles » lors de l'utilisation d'appareils privés à des fins professionnelles. d. imposer 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. e. clairement identifier les appareils mobiles propres, doit les configurer en toute sécurité (et les équiper des logiciels antimalware nécessaires ainsi que des logiciels permettant la suppression à distance de l'ensemble des données sur l'appareil) et doit conserver leur identification dans un registre central. f. prévoir les contrôles appropriés[7] afin de vérifier la conformité des appareils mobiles par rapport aux directives relatives 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). L'organisation n'est pas responsable pour les dommages ou frais qu'entraîne la perte ou le vol de données privées. g. régulièrement sensibiliser 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). h. avoir la possibilité de bloquer directement l'accès aux informations de l'organisation (données ou applications présentes sur l'appareil mobile) et d'effacer les données. i. s'engager à respecter la vie privée de l'utilisateur.
5.3.2.2	Télétravail sécurisé	Toute organisation doit a. prendre les mesures adéquates, en fonction du moyen d'accès[8], afin de garantir la sécurité de l'information de l'accès en ligne réalisé en dehors de l'organisation aux données sensibles, confidentielles et professionnelles de l'organisation. b. clairement définir des règles de bonne conduite ainsi qu'une mise en œuvre appropriée du télétravail, doit les valider, les communiquer et les tenir à jour, et 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.

6 Moyen d'accès: p.ex. Internet, ligne louée, réseau privé, réseau sans fil.

7 Toujours sur la base d'un accord réciproque entre l'organisation et l'utilisateur.

8 Moyen d'accès: p.ex. Internet, ligne louée, réseau privé, réseau sans fil.

	Objet	Norme minimale
		c. organiser 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'organisation au départ du lieu de télétravail.

5.4. Sécurité liée aux collaborateurs (Clean desk & Clear desk)

	Objet	Norme minimale
5.4.1	Rapportage, évaluation et campagne de sensibilisation	Toute organisation doit • au moins une fois par an, organiser une campagne de sensibilisation ou une session d'information relative à la sécurité de l'information et à la vie privée, la valider, la communiquer et en assurer le suivi. • réaliser une évaluation annuelle du respect de la présente politique dans la pratique (au moyen d'une enquête interne).
5.4.2	Accès à l'information	Toute organisation doit a. élaborer une directive stipulant que la collaboration de l'ensemble des collaborateurs est essentielle pour la sécurité de l'information et la vie privée. Tout collaborateur joue un rôle crucial pour empêcher tout accès illicite aux informations sensibles. Ceci est valable tant pour les accès aux systèmes d'information et aux applications que pour l'accès physique aux locaux ou aux documents. b. élaborer une directive stipulant que l'utilisateur demeure responsable des informations, quelle que soit la forme sous laquelle ces informations sont enregistrées. L'utilisateur doit donc veiller à la bonne protection de celles-ci. Dès que les informations ne sont plus utilisées par l'utilisateur, ce dernier doit aussi veiller à leur archivage ou à leur destruction. c. Implémenter un système d'accès (physique ou logique) afin d'éviter tout accès non autorisé à l'organisation. L'accès est sécurisé par un dispositif d'accès précis.

5.5. Gestion des actifs

	Sujet	Norme minimale
5.5.1	Classification des données	Toute organisation doit a. appliquer une protection ou une classification des informations prévue, en ce compris les mesures relatives à la sécurité de l'information et à la vie privée y afférentes, selon un schéma de classification interne qui est conforme à la législation spécifique en la matière et à la réglementation internationale[9]. b. mettre au point des procédures appropriées et des registres, les valider, les mettre en œuvre, les communiquer et les tenir à jour en vue de la labellisation (étiquetage) et du traitement de l'ensemble des collectes de

[9] en particulier la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité.

	Sujet	Norme minimale
		données, supports de données et systèmes d'information en cours de gestion, et ce conformément au schéma de classification interne. c. appliquer la règle selon laquelle la classification définie par ce type d'information vaut également pour le niveau supérieur des systèmes d'information, c'est-à-dire que si un système traite des informations secrètes, l'ensemble du système est considéré comme secret, sauf si des mesures ont été prises au sein de ce système d'information pour ce niveau supérieur. d. Les classifications de tous les systèmes critiques doivent toutes être définies à un niveau central par leurs propriétaires. e. Les classifications de tous les systèmes critiques doivent être contrôlées annuellement par le conseiller en sécurité de l'information (CISO) et/ou le délégué à la protection des données (DPO). f. rendre les mesures de contrôle conformes aux risques, tout en tenant compte des possibilités techniques et du coût des mesures à prendre.
5.5.2	Inventaire	Toute organisation doit disposer d'un inventaire du matériel informatique et des logiciels qui est mis à jour en permanence.
5.5.3	Protection des actifs de l'entreprise	Toute organisation doit s'assurer que les supports des données à caractère personnel et les systèmes informatiques les traitant[10], sont placés, conformément à leur classification, dans des locaux identifiés et protégés. L'accès à ces locaux est limité aux seules personnes autorisées et aux seules heures justifiées par leur fonction.
5.5.4	E-mail, communication en ligne et utilisation d'internet	Toute organisation doit : a. intégrer dans sa directive 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 ». Ces règles sont décrites dans les paragraphes: • utilisation de l'e-mail et des moyens de communication en ligne • utilisation sécurisée de l'internet b. exercer 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.
5.5.5	Support physique en transit	Toute organisation doit prendre les mesures nécessaires pour protéger, contre les accès non autorisés, les supports en transit, notamment les backups contenant des données sensibles.

[10] Par "traitement", on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion.

5.6. Protection de l'accès (logique)

	Sujet	Norme minimale
5.6.1	Gestion des accès aux portails	Toute organisation qui souhaite utiliser les services et applications du portail de la sécurité sociale pour les besoins de ses utilisateurs doit: a. désigner au moins un gestionnaire des accès b. stimuler ses collaborateurs à lire et à appliquer les règlements relatifs à l'utilisation des systèmes d'information des portails. c. respecter les obligations liées à l'exercice de la fonction de gestionnaire ou de co-gestionnaire qui sont décrites dans la politique « gestion sécurisée des accès aux portails »
5.6.2	Accès au réseau de la BCSS via internet	Toute organisation doit : • demander une autorisation et une dérogation écrites au fonctionnaire dirigeant de la BCSS lorsqu'elle souhaite utiliser l'internet comme moyen d'accès au réseau de la Banque Carrefour de la sécurité sociale (BCSS). L'utilisation de l'internet comme moyen d'accès au réseau de la Banque Carrefour de la sécurité sociale (BCSS) constitue une exception au principe général de l'accès via l'Extranet de la sécurité sociale. • le contenu de la demande d'autorisation et de dérogation doit satisfaire aux spécifications mentionnées dans le paragraphe « contenu de la demande » de la politique « Utilisation d'internet pour accéder 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 » • également, lorsqu'elle souhaite utiliser l'internet comme moyen d'accès au réseau de la Banque Carrefour de la sécurité sociale (BCSS), appliquer strictement les conditions énumérées à l'annexe D (Conditions d'accès à l'Extranet de la sécurité sociale via internet) de la politique. Ces conditions portent sur: ○ le niveau des autorisations d'accès ○ le niveau d'identification/authentification ○ la traçabilité ○ les restrictions ○ la connexion via transfert de fichiers
5.6.3	Protection des données	Toute organisation doit sécuriser l'accès aux données[11] nécessaires à l'application et à l'exécution de la sécurité sociale par un système d'identification, d'authentification et d'autorisation.
5.6.4	Autorisations comité sectoriel	Toute organisation doit s'assurer de l'existence des autorisations nécessaires du comité sectoriel compétent pour l'accès aux données (sociales) à caractère personnel gérées par une autre organisation.

11 Dans la présente norme, on entend par le terme "donnée" non seulement les données sociales à caractère personnel mais aussi tous les éléments logiques du système d'information qui assurent le traitement ; par exemple les programmes, les applications, les fichiers, les utilitaires de système et autres éléments du système d'exploitation.

	Sujet	Norme minimale
5.6.5	Accès aux systèmes informatiques par les gestionnaires d'information [12]	Toute organisation doit limiter l'accès au(x) système(s) informatique(s) aux gestionnaires d'information identifiés, authentifiés et autorisés.
5.6.6	Utilisation des services en réseaux	Toute organisation doit prendre les mesures adéquates afin que toute personne ait uniquement accès aux services pour lesquels elle a spécifiquement reçu une autorisation.
5.6.7	Connexion IP externe - réseau primaire	Toute institution de sécurité sociale du réseau primaire doit utiliser l'Extranet de la sécurité sociale[13] pour l'ensemble de ses connexions externes ou pour les connexions avec son réseau secondaire.[14] Toute dérogation à cette mesure doit faire l'objet d'une demande motivée qui devra être introduite par l'intermédiaire du service de sécurité de la BCSS.
5.6.8	Connexion IP externe - réseau secondaire	Toute organisation appartenant à un réseau secondaire peut utiliser l'Extranet de la sécurité sociale pour ses connexions externes à la sécurité sociale. Dans le cas où l'organisation se connecte aux réseaux externes sans passer par l'Extranet de la sécurité sociale : • l'organisation concernée doit prendre les mesures de sécurité qui garantiront un niveau de sécurité équivalent à celui de l'Extranet de la sécurité sociale pour les systèmes informatiques utilisés pour le traitement de données à caractère personnel ; • l'institution gérant le réseau secondaire concerné doit prendre les mesures de sécurité qui garantiront un niveau de sécurité équivalent à celui de l'Extranet de la sécurité sociale.

5.7. Chiffrement

	Objet	Norme minimale
5.7.1	Chiffrement	Toute organisation doit : • définir une politique formelle pour l'utilisation de contrôles cryptographiques, la valider, la communiquer et la tenir à jour. A cet effet, elle doit utiliser les « Directives relatives à l'utilisation de contrôles cryptographiques » qui sont énumérées dans l'annexe C de la politique « chiffrement ». • définir, pour le cycle de vie complet, une politique formelle pour l'utilisation, la protection et la durée de vie des clés cryptographiques, la valider, la

12 Le gestionnaire d'information est toute personne qui dispose, dans le cadre de ses responsabilités en matière de système ICT, de droits d'accès plus larges que la simple utilisation fonctionnelle des données. Il s'agit entre autres des développeurs, des gestionnaires système, des gestionnaires de données, des développeurs et gestionnaires de logiciels, des gestionnaires de réseau, des consultants et des sous-traitants.

13 L'Extranet de la sécurité sociale est le support technique permettant l'échange informatisé de données dans le cadre du réseau Banque Carrefour de la sécurité sociale. (Les informations complémentaires sur l'Extranet sont disponibles sur le site de la Banque Carrefour de la sécurité sociale)

14 Cette mesure n'est pas d'application pour les systèmes informatiques qui ne sont pas utilisés pour le traitement des données sociales à caractère personnel et qui ne sont en aucune façon reliés aux systèmes informatiques utilisés pour le traitement de données sociales à caractère personnel.

	Objet	Norme minimale
		communiquer et la tenir à jour. A cet effet, elle doit utiliser les « Directives relatives à la gestion des clés » qui sont énumérées dans l'annexe D de la politique « chiffrement ».

5.8. Protection physique et protection de l'environnement

	Sujet	Norme minimale
5.8.1	Espaces sécurisés	Toute organisation doit limiter l'accès aux bâtiments et locaux aux personnes autorisées et effectuer un contrôle à ce sujet tant pendant qu'en dehors des heures de travail. a. Il y a lieu de prévoir des dispositifs de protection des accès (barrières telles des murs, des portes d'accès avec des clés sous format de cartes ou une réception avec personnel) afin de protéger les espaces de stockage d'informations sensibles ou critiques ou d'équipements TIC. b. Les zones d'un bâtiment accessibles à titre privé ainsi que les espaces sécurisés doivent être protégés par une protection des accès adéquate, afin de garantir que seul le personnel compétent puisse y accéder. c. Il y a lieu de concevoir et de réaliser une protection physique des bureaux, des espaces et des facilités. d. Toute organisation doit prendre des mesures pour la prévention, la protection, la détection, l'extinction et l'intervention en cas d'incendie, d'intrusion et de dégâts causés par l'eau. e. Il y a lieu de concevoir et de réaliser une protection physique et des directives pour les travaux à réaliser dans des espaces sécurisés. f. Les points d'accès tels les espaces de chargement et de déchargement qui sont accessibles à des personnes non autorisées, doivent être maîtrisés et, si possible, être protégés par des dispositifs critiques et/ou des dispositifs TIC afin d'éviter tout accès non autorisé
5.8.2	Protection des appareils	Toute organisation doit prendre des mesures de prévention contre la perte, l'endommagement, le vol ou la compromission des actifs de l'entreprise et contre l'interruption des activités de l'entreprise. a. Les appareils critiques doivent être placés et protégés de la sorte que les risques d'endommagement et de dysfonctionnement par l'extérieur et la possibilité d'accès par des personnes non autorisées soient réduits. b. Toute organisation doit disposer d'un moyen alternatif en électricité afin de garantir la prestation de services attendue. Les appareils critiques doivent être protégés contre une interruption du courant et autres pannes par une interruption des équipements d'utilité publique. c. Les câbles d'alimentation ou de télécommunication utilisés pour les échanges de données ou les services d'information d'appui doivent être protégés contre toute interception ou tout endommagement. d. Les appareils critiques doivent être maintenus correctement, de sorte qu'ils soient disponibles en permanence et se trouvent en bon état de fonctionnement. e. Les appareils, les informations et les programmes de l'organisation ne peuvent pas être déplacés sans l'accord préalable.

	Sujet	Norme minimale
		f. Les appareils situés à l'extérieur doivent être protégés, tout en tenant compte des risques divers engendrés par des travaux en dehors du terrain de l'organisation g. Toute organisation doit prendre les mesures utiles pour que l'ensemble des données soient supprimées ou rendues inaccessibles sur tout support de stockage avant sa mise au rebut ou son recyclage. h. Les utilisateurs doivent garantir que les appareils sans surveillance sont protégés de manière adéquate.
5.8.3	Suppression des supports d'information électroniques	Toute organisation: a. en cas d'utilisation du chiffrement comme mesure de base préventive contre le vol, l'abus ou la perte du support d'information • ne peut jamais apposer les clés de chiffrement de manière visible sur le support même. • Le chiffrement doit avoir trait à des volumes logiques dans leur ensemble (au lieu de fichiers ou de répertoires individuels). • Le chiffrement sert de complément aux mesures applicables sur le plan de l'organisation et aux procédures visant à prévenir des abus. b. en cas de réutilisation du support d'information, doit réutiliser celui-ci dans un niveau de classification des données au moins comparable. c. Doit réaliser une évaluation des risques, afin de déterminer la méthode appropriée[15] pour la suppression du support d'information. d. en cas de la présence d'un risque résiduel[16] de retrouver des données consécutivement à la suppression, qui n'est pas acceptable pour l'organisation, doit détruire physiquement le support d'information, même si le risque résiduel est hypothétique. e. doit déterminer contractuellement les mesures appropriées pour la suppression de données lorsque • l'organisation utilise des supports de données qui ne sont pas sa propriété (par exemple, dans le cadre du leasing ou du disaster recovery) • l'organisation ne maîtrise pas la technologie d'accès à l'ensemble des niveaux du support d'information (par exemple, dans le cadre du cloud computing).

5.9. Gestion opérationnelle

	Sujet	Norme minimale
5.9.1	Séparation des environnements	Toute organisation doit s'assurer que tout développement ou test est exclu au sein de l'environnement de production. Dans certains cas exceptionnels, ces tests peuvent déroger à la règle moyennant la mise en place de mesures adéquates.

[15] Voir l'annexe D de la politique 'suppression des supports d'information électroniques'

[16] La probabilité d'un impact négatif, malgré les mesures prises pour influencer (limiter) le risque (inhérent)

	Sujet	Norme minimale
5.9.2	La gestion de la mise en production	Toute organisation doit : • disposer de procédures pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes • éviter qu'une seule et même personne n'assure le contrôle de l'ensemble de ce processus.
5.9.3	Protection contre des codes nocifs[17]	Toute organisation doit disposer de systèmes actualisés pour se protéger (prévention, détection et rétablissement) contre des codes nocifs.
5.9.4	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 5.14.). • contrôler régulièrement les sauvegardes réalisées dans ce cadre.
5.9.5	Journalisation des accès	Toute organisation doit : • définir une procédure de journalisation formelle, la valider, la communiquer et la tenir à jour. • définir de manière structurée, dans des fichiers de journalisation individuels, les transactions, les travaux de contrôle, les activités des utilisateurs, les exceptions et les événements liés à la sécurité de l'information et à la vie privée, de sorte que toute action puisse être mise en rapport avec les documents source et que toute opération effectuée puisse être contrôlée. • La journalisation doit être 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 ». • Tout accès à des données personnelles et confidentielles à caractère social ou médical doit faire l'objet d'une prise de traces, conformément à la législation et à la réglementation applicables. • Les horloges internes de l'ensemble des systèmes d'information de l'organisation doivent être synchronisées avec une source temporelle précise et déterminée, de sorte qu'une analyse fiable des fichiers de journalisation sur les différents systèmes d'information soit toujours possible. • Les outils nécessaires doivent être disponibles ou être développés que sorte que les données de journalisation puissent être analysées par les personnes autorisées. • L'utilisation du système doit, dans la mesure du possible, faire l'objet d'une prise de traces automatique. Si cela n'est pas possible, les gestionnaires de système peuvent également tenir un journal manuel. • Les fichiers de journalisation doivent être protégés contre toute consultation par des personnes non autorisées, toute modification ou toute suppression. • Les fichiers de journalisation doivent être conservés pendant une période convenue, pour les investigations et contrôles futurs et ce en conformité avec la législation et la réglementation[18].

17 Codes malveillants: p.ex. virus, ver, cheval de Troie, spam, spyware.

	Sujet	Norme minimale
		• La consultation des fichiers de journalisation doit toujours faire l'objet d'une procédure organisée au sein de l'organisation qui tient à jour un historique des demandées approuvées/exécutées ou refusées. • Le résultat de la journalisation doit être analysé, rapporté et évalué à des intervalles réguliers.
5.9.6	Traçabilité des identités.	Chaque organisation participant à la transmission de données au travers de la Banque Carrefour est tenue d'assurer à son niveau la traçabilité des identifiants utilisés. Cette traçabilité doit permettre l'identification de bout en bout des identifiants utilisés[19].
5.9.7	Détection d'infractions à la sécurité	Toute organisation 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 proportionnellement au risque technique / opérationnel.

5.10. Sécurité des communications

	Sujet	Norme minimale
5.10.1	Réseaux sans fil sécurisés	Toute organisation doit pour l'ensemble des réseaux sans fil qu'il a sous sa gestion et à tous les endroits: a. gérer et contrôler les réseaux sans fil afin de limiter l'accès au réseau et l'utilisation du réseau et afin de protéger les informations présentes dans les systèmes et applications qui sont envoyées à travers des réseaux sans fil b. respecter les directives qui sont décrites dans l'annexe C de la politique « réseaux sans fil sécurisés »
5.10.2	Gestion de la sécurité du réseau	Toute organisation doit vérifier que les réseaux sont gérés et contrôlés de façon adéquate afin de les protéger contre les menaces et de garantir de façon efficace la protection des systèmes et des applications qui utilisent le réseau.
5.10.3	Disponibilité du réseau	Toute organisation doit mettre 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. Par voie de conséquence, cela présuppose que cette connexion doit être au minimum dédoublée vers plusieurs nœuds de l'Extranet.
5.10.4	Cartographie des flux de l'extranet	Toute organisation doit tenir à jour une cartographie technique[20] des flux implémentés au travers de l'Extranet de la sécurité sociale et en informer le conseiller en sécurité.
5.10.5	Qualité de service des	Chaque transfert d'informations à caractère social au sein du réseau de la sécurité

[18] Telle le RGPD UE

[19] Par exemple, lorsque dans la zone « USERID » de la partie préfixe d'un message qu'elle adresse à la Banque Carrefour, l'institution reprend le numéro du programme qui a généré le message bien qu'une personne physique soit à l'origine du message, la Banque Carrefour peut, a posteriori, retrouver ce numéro de 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 à l'institution de sécurité sociale de faire la relation entre le numéro de programme qu'elle reprend dans la partie préfixe du message adressé à la Banque Carrefour et l'identité de la personne physique qui émet le message.

20 Les flux techniques au niveau du réseau sont nécessaires à la gestion des firewalls dans les différentes zones de l'Extranet.

	Sujet	Norme minimale
	échanges d'informations à caractère social	sociale doit être traité dans les meilleurs délais par l'ensemble des intervenants, qu'ils soient intermédiaires ou destinataires/récepteurs. Les institutions qui transmettent des informations à caractère social au sein du réseau de la sécurité sociale, particulièrement lorsqu'elles sont la source authentique, doivent traiter en temps utile les messages de suivi qu'elles doivent recevoir des destinataires ou intermédiaires. Chaque acteur, tant destinataire/récepteur qu'intermédiaire ou émetteur, participant à la transmission est tenu d'entreprendre dans les meilleurs délais les actions adéquates et appropriées consécutives au traitement des messages de suivi. Toute anomalie ou lacune dans la transmission électronique des données doit être signalée dans les meilleurs délais aux intervenants concernés, qu'ils soient récepteurs, intermédiaires, ou émetteurs.

5.11. Achat, conception, développement et maintenance d'applications

	Objet	Norme minimale
5.11.1	Communication	Toute organisation doit mettre au point une communication efficace et constructive entre les différentes parties concernées par le projet (en ce compris avec les clients et les fournisseurs), en particulier avec le(s) conseiller(s) en sécurité. Ceci doit garantir un niveau adéquat de sécurité de l'information et de vie privée qui est connu par tous.
5.11.2	Gestion des accès	Toute organisation doit : a. faire travailler l'ensemble des collaborateurs avec des moyens TIC (mis à la disposition par l'organisation) sur la base d'une autorisation minimale pour l'exécution de leurs tâches. b. Lors du développement de la protection des accès, tenir compte des systèmes opérationnels existants de gestion des accès (tels l'UAM) et de leur évolution. c. définir, documenter, valider et communiquer les conditions de protection des accès (identification, authentification, autorisation). Ces accès font l'objet d'une prise de traces. d. Il y a lieu d'éviter dans toute la mesure du possible la gestion des accès dans une application. Dans des cas exceptionnels, il faut disposer de procédures formelles permettant de gérer l'ensemble des phases du cycle de vie de la protection des accès (introduction, contrôle sur la base d'un inventaire, mutation, suppression). e. 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 organisation doit être en mesure d'établir elle-même la relation entre ce numéro de programme et l'identité de la personne physique qui envoie ce message.
5.11.3	Sous-traitance à des tiers	Toute organisation doit fixer, dans un contrat, les risques relatifs à la sécurité et à la vie privée et doit prévoir une clause de confidentialité et de continuité.
5.11.4	Check-list	Toute organisation doit toujours prévoir une liste de contrôle pour le chef de

	Objet	Norme minimale
		projet de sorte que le chef de projet 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 projet.
5.11.5	Contrôle de la mise en production	Toute organisation doit s'assurer par l'entremise du responsable du suivi, le chef de projet, et 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.
5.11.6	Approche structurée	Toute organisation doit, sous la supervision du chef de projet, scinder les dispositifs de développement, de test et/ou d'acceptation, et de production - en ce compris veiller à la séparation y liée en ce qui concerne les responsabilités dans le cadre du projet.
5.11.7	Gestion des traces au cours d'un projet	Toute organisation doit : a. journaliser chaque accès à des données personnelles et confidentielles à caractère social ou médical, conformément à la politique « journalisation » et à la législation et à la réglementation applicables. b. préciser, dans les spécifications d'un projet, comment l'accès et l'utilisation des systèmes et des applications seront journalisés, afin de contribuer à la détection d'anomalies par rapport aux directives relatives à la sécurité de l'information et à la vie privée. La journalisation doit au moins satisfaire aux objectifs suivants: a. pouvoir déterminer rapidement, en toute simplicité et de manière limpide qui a obtenu accès à quelles informations, à quel moment et de quelle manière b. l'identification de la nature des informations consultées c. l'identification précise de la personne c. tenir compte des systèmes de journalisation existants lors de l'évaluation des besoins de journalisation dans le cadre du présent projet. d. développer ou mettre les outils nécessaires à la disposition afin de permettre l'exploitation de ces données de journalisation par les personnes autorisées. e. appliquer la règle générale selon laquelle les données de journalisation fonctionnelles/transactionnelles doivent être conservées pendant 10 ans au moins et les données de journalisation techniques/infrastructurelles pendant 2 ans au moins.
5.11.8	Back-up/Restore	Toute organisation doit intégrer les déliverables du projet dans un système de gestion des sauvegardes de l'organisation comme imposé dans la politique. Ceci concerne non seulement les données qui sont traitées mais aussi la documentation qui y a trait (code source, programmes, documents techniques, ...). La sauvegarde doit régulièrement être testée au moyen d'un exercice de restauration (« restore ») afin de vérifier que les informations peuvent effectivement être récupérées et quel est le délai nécessaire pour cette mission de reprise.
5.11.9	Gestion de la continuité au cours d'un projet	Toute organisation doit : a. Au cours du développement du projet, formaliser les besoins relatifs à la

	Objet	Norme minimale
		continuité de la prestation de services, conformément aux attentes de l'organisation. b. Intégrer clairement dans les programmes, les points de reprise à définir afin de faire face à des problèmes opérationnels. Ces informations font partie du dossier d'exploitation. c. Au cours du développement d'un projet, accorder une attention spécifique à une sauvegarde et à une restauration (« restore ») des informations. d. Dans l'environnement de production, tenir compte des exigences de l'institution en ce qui concerne la tolérance aux problèmes et la redondance de l'infrastructure e. Actualiser le plan de continuité et les procédures y afférentes en fonction de l'évolution du projet, en ce compris les tests de continuité f. Exécuter une analyse des risques au début du projet afin de définir les procédures d'urgence. Celles-ci doivent comprendre: • Le fonctionnement en cas de disponibilité réduite des systèmes d'information • La description de systèmes d'information alternatifs, en ce compris le déploiement, les modalités d'exploitation et le développement éventuel de systèmes d'urgence • Les tâches et procédures clés en cas d'interruption du système • Les tâches, les rôles clés et les moyens à mettre en œuvre afin de garantir une disponibilité optimale.
5.11.10	Gestion des incidents au cours d'un projet	Toute organisation doit : a. Au cours du développement d'un projet, formaliser et valider les procédures relatives à la gestion des incidents. Ceci doit permettre d'intégrer le système développé dans le système de gestion standard des incidents de l'organisation. b. Le conseiller en sécurité doit être informé des incidents concernant la sécurité et la vie privée au cours du développement d'un projet.
5.11.11	Documentation	Toute organisation doit actualiser la documentation (technique, procédures, manuels, ...) au cours de la durée de vie du projet.
5.11.12	Inventaire	Toute organisation doit ajouter tous les actifs, en ce compris les systèmes acquis ou développés, au système de gestion des moyens opérationnels.
5.11.13	Audit	Toute organisation doit, à des fins d'audit interne et externe, apporter la collaboration appropriée sous la forme de mise à la disposition du personnel, de la documentation, de la la journalisation et des autres informations qui sont raisonnablement disponibles.
5.11.14	Sécurité du cycle de vie du projet	Toute organisation doit appliquer le « secure project lifecycle » tel que décrit à l'annexe C de la politique « Achat, conception, développement et maintenance d'applications ».
5.11.15	Sécurité applicative	Toute organisation doit prendre les mesures nécessaires pour assurer la sécurité au niveau applicatif dans le but de minimiser les brèches potentielles en matière de sécurité de l'information (confidentialité, intégrité, disponibilité)[21].

21 Des exemples de cette menace sont: SQL injection, Spoofing, Cross Site Scripting, Elevation Privilege (Top Ten OWASP).

5.12. Relations avec les fournisseurs

	Objet	Norme minimale
5.12.1	Sécurité de la sous-traitance à des tiers	En cas de sous-traitance, toute organisation doit s'assurer que: a. les obligations[22] en matière de traitement de données à caractère personnel sont contractuellement établies. b. les conditions relatives à la sécurité de l'information et à la vie privée font l'objet d'un accord avec les tiers et sont documentées afin de réduire les risques relatifs à l'accès des tiers aux moyens d'information c. toutes les conditions pertinentes relatives à la sécurité de l'information et à la vie privée font l'objet d'un accord avec chacun de ces tiers qui lisent, traitent, enregistrent, communiquent les informations de l'organisation ou fournissent des éléments d'infrastructure TIC d. les contrats conclus avec les tiers comprennent 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 TIC e. l'organisation doit régulièrement effectuer un monitoring de la prestation de service de tiers et doit évaluer et auditer cette prestation de service f. gérer les adaptations de la prestation de service par des tiers, dont notamment l'actualisation et l'amélioration des politiques, procédures et mesures relatives à la sécurité de l'information et à la vie privée existantes. Lors de la gestion, il y a lieu de tenir compte du caractère critique des systèmes et processus en question et de la réévaluation des risques g. appliquer les « directives relatives à la sécurité de la sous-traitance à des tiers » telles que décrites dans l'annexe C de la politique « sécurité de la sous-traitance à des tiers ».
5.12.2	Cloud computing	Toute organisation doit : a. lorsqu'elle fait appel aux services d'un cloud, conformément au point 2.1 de la politique « Cloud computing » b. lorsqu'elle souhaite traiter des données sensibles, confidentielles ou professionnelles dans un cloud ○ respecter les garanties contractuelles minimales telles que décrites au point 2.2 de la politique « Cloud computing » ○ respecter la sécurité de l'information du fournisseur du cloud telle que précisée au point 2.3 de la politique « Cloud computing » ○ respecter la vie privée du fournisseur du cloud telle que précisée au point 2.4 de la politique « Cloud computing »

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

	Sujet	Norme minimale

22 L'organisation demeure responsable de la sécurité de l'information et de la vie privée du traitement, y compris du traitement chez le(s) sous-traitant(s).

	Sujet	Norme minimale
5.13.1	Gestion des incidents	Toute organisation doit : a. Disposer 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 y afférentes. Ces procédures doivent être connues par tous les collaborateurs. b. Fixer dans un contrat avec les collaborateurs 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. c. Rendre publics 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, de sorte que l'organisation puisse prendre, en temps utile, des mesures correctrices adéquates. d. Rapporter les incidents relatifs à la sécurité de l'information et à la vie privée, dans les meilleurs délais, à l'intervention du supérieur hiérarchique, du helpdesk, du conseiller en sécurité de l'information (CISO) ou du délégué à la protection des données (DPO). e. En cas d'incidents relatifs à la sécurité de l'information ou à la vie privée, collecter correctement les preuves conformément aux prescriptions réglementaires et légales. f. Tout incident relatif à la sécurité de l'information ou à la vie privée doit être évalué de manière formelle, de sorte que les procédures et mesures de contrôle puissent être améliorées. Les leçons tirées d'un incident doivent être communiquées à la direction de l'organisation, en vue de la validation et de l'approbation d'actions futures. g. appliquer la « directive relative à la gestion des incidents » telle que décrite dans l'annexe C de la politique « Gestion des incidents »

5.14. Aspects de la sécurité de l'information dans la gestion de la continuité

	Objet	Norme minimale
5.14.1	Gestion de la continuité	Toute organisation doit : a. Rédiger un plan de continuité pour tous les processus critiques et systèmes d'information essentiels. Ce plan décrit l'ensemble des activités, mesures et données essentielles des processus de l'organisation, ayant pour but de limiter le temps d'interruption à un niveau acceptable. b. Élaborer la sécurité de l'information et la vie privée comme faisant intégralement partie de la gestion de la continuité (voir l'annexe C « Directives relatives à la continuité de la sécurité de l'information et de la vie privée » de la politique « Gestion de la continuité ») c. Disposer d'un plan de continuité propre qui accorde au moins une attention à: 1) L'identification et à la documentation des processus essentiels et des systèmes d'information y afférents de l'organisation; 2) L'évaluation des risques dans laquelle le risque, l'impact et les mesures de contrôle actuelles sont définies; 3) Les connaissances et compétences des collaborateurs leur permettant de faire tourner les processus essentiels et systèmes d'information y

	Objet	Norme minimale
		afférents ou de les redémarrer; 4) En cas d'incident grave ou de sinistre, qui peut activer le plan de continuité, quand et comment? 5) Informations (acceptabilité de la perte d'information); 6) Priorités et ordre de restauration; 7) Communication pendant et après un incident grave ou un sinistre; 8) Comment le plan de continuité exécuté est-il formellement clôturé après un incident grave ou un sinistre, par qui et à quel moment? d. Disposer d'une gestion de la continuité adéquate qui limite l'impact d'un incident grave ou d'un sinistre et sa restauration à un niveau acceptable, et ce conformément aux attentes de l'organisation. e. Régulièrement tester et adapter le plan de continuité. Les résultats des tests doivent être communiqués à la direction de l'organisation en vue de la validation et de l'approbation d'actions futures.

5.15. Respect

	Objet	Norme minimale
5.15.1	Respect	Toute organisation doit : a. réaliser 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[23]. b. éviter toute violation de la législation et des obligations contractuelles, statutaires, réglementaires ou légales relatives à la sécurité de l'information et à la vie privée. c. garantir que la sécurité de l'information et la vie privée ont été mises en œuvre et sont opérationnelles conformément aux attentes de la direction. d. disposer d'un procédure disciplinaire formelle pour les travailleurs ayant commis une infraction à la sécurité de l'information ou à la vie privée. e. appliquer la « directive relative au respect » (annexe C de la politique « respect »).
5.15.2	Traitement de données à caractère personnel	Toute organisation doit : a. régulièrement dresser la carte des risques relatifs à la conformité au Règlement européen[24]. Les actions planifiées suite à un risque « résiduel » majeur de non-conformité doivent être intégrées dans le plan de l'organisation relatif à la sécurité de l'information et à la vie privée. b. En fonction du rôle (sous-traitant ou responsable du traitement) pour un traitement spécifique (ou groupe de traitements spécifiques), au moins réaliser les actions suivantes:

23 Selon les bonnes pratiques en vigueur, cet audit devrait être organisé au moins une fois par an. Qui plus est, il n'est pas interdit qu'un conseiller en sécurité d'une organisation audite une autre organisation d'un même réseau. Dans le cas où une institution gestionnaire d'un réseau secondaire se trouve confrontée à un manque de vision par rapport à la situation de la sécurité de l'information ou relative à la vie privée de l'un de ses membres, celle-ci pourra demander au Comité sectoriel de réaliser un audit de conformité.

24 https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_NL.pdf

	Objet	Norme minimale
		• inscrire le traitement dans le registre central des responsables de traitement ou des sous-traitants; • une justification formelle de la non-réalisation des mesures de contrôle axées sur le respect du Règlement européen[25].

6. Maintien, suivi et révision

Un questionnaire sera transmis annuellement aux organisations du réseau de la sécurité sociale en vue de l'évaluation du respect des normes minimales relatives à la sécurité de l'information et à la vie privée et de l'examen de remarques.

Sur base des questionnaires complétés qui lui sont transmis, le Comité sectoriel de la sécurité sociale et de la santé peut faire effectuer des contrôles concernant le respect de certains points spécifiques des normes minimales relatives à la sécurité de l'information et à la vie privée dans une organisation.

Une modification des normes minimales relatives à la sécurité de l'information et à la vie privée donne lieu à

- la soumission de la proposition de modification au Comité sectoriel de la sécurité sociale et de la santé;
- la soumission du questionnaire modifié au Comité sectoriel de la sécurité sociale et de la santé;
- l'envoi des normes minimales de sécurité modifiés et approuvés aux responsables de la gestion journalière des organisations qui en informent leur Comité de gestion ;
- l'entrée en vigueur des normes minimales approuvées dans l'année suivant leur approbation par le Comité de gestion[26] de la Banque Carrefour de la sécurité sociale (BCSS).

Les aspects faisant l'objet de mesures spécifiques qui ont été approuvées au niveau du Comité général de coordination[27] mais qui ne sont pas encore reprises dans une version révisée des normes minimales relatives à la sécurité de l'information et à la vie privée, seront repris de façon proactive dans le questionnaire annuel.

7. Sanction

Au vu des manquements constatés dans le respect de ces normes minimales relatives à la sécurité de l'information et à la vie privée par une organisation, le Comité sectoriel peut inviter la Banque Carrefour de la sécurité sociale (BCSS) à ne plus donner suite aux soumissions adressées par cette organisation. Avant de prendre cette mesure, le Comité sectoriel de la sécurité sociale et de la santé entendra la personne chargée de la gestion journalière de l'organisation concernée.

[25] appliquer ou expliquer principe ("comply or explain principle")

[26] Le Comité de gestion donne les instructions utiles relatives à l'application de la loi relative à la BCSS et rend des avis sur les propositions de modifications aux lois et aux arrêtés royaux qui concernent la Banque Carrefour de la sécurité sociale et le fonctionnement du réseau de la sécurité sociale. Le Ministre de tutelle consulte le Comité de gestion sur toutes les matières qu'il juge utile.

[27] Le Comité général de coordination assiste le Comité de gestion de la Banque Carrefour de la sécurité sociale (BCSS) et le Comité sectoriel de la sécurité sociale et de la santé dans l'accomplissement de leurs missions. A cet effet, il est chargé de proposer toute initiative de nature à promouvoir et à consolider la collaboration au sein du réseau ainsi que toute mesure pouvant contribuer à un traitement légal et confidentiel des données sociales à caractère personnel. »

ANNEXE A: Politiques relatives à la sécurité de l'information et à la vie privée applicables (version 2017)

Ci-après figure une liste des politiques davantage détaillées telles que choisies par le groupe de travail Sécurité de l'information. Pour les institutions en général, pour les responsables, pour les sous-traitants des informations, pour le conseiller en sécurité de l'information (CISO) et pour le délégué à la protection des données (DPO), ces politiques constituent une source d'inspiration supplémentaire sur lesquelles ils peuvent se baser lors de l'exécution de leurs missions relatives à la sécurité de l'information et à la vie privée. L'application de ces politiques relèvent cependant de la responsabilité de toute institution. Toute organisation peut elle-même suggérer et/ou élaborer des politiques supplémentaires.

Cette liste n'est pas exhaustive et sera régulièrement mise à jour.

BLD RISK	**Evaluation des risques**
BLD HR	**Aspects liés aux personnes**
BLD DATA	**Classification des données**
BLD DESK	**Clean and Clear Desk**
BLD TELE	**Télétravail**
BLD ONLINE	**E-mail, outils de communication en ligne et utilisation d'Internet**
BLD WIREL	**Réseaux sans fil**
BLD BCSS	**Utilisation de l'Internet pour accéder au réseau de la BCSS dans le cadre du traitement de données à caractère personnel par les acteurs du secteur social**
BLD PORTAL	**Gestion des accès aux portails**
BLD CRYPT	**Chiffrement**
BLD AUTH	**Définition du moyen d'authentification pour l'application**
BLD DATA SEC	**Sécurité des données**
BLD PHYS	**Protection physique de l'accès**
BLD ERASE	**Suppression de supports d'information**
BLD LOG	**Gestion des logs**
BLD MOBILE	**Appareils mobiles**
BLD APPDEV	**Achat, conception, développement et la maintenance de systèmes d'information**
BLD OUTS	**Sous-traitance à des tiers**
BLD CLOUD	**Cloud**
BLD INCID	**Gestion des incidents**
BLD BCM	**Gestion de la continuité**
BLD COMPLY	**Respect**
BLD PRIV	**Traitement de données personnelles**

***** FIN DU DOCUMENT *****