Politique de sécurité de l'information et protection de la vie privée

Aspects liés aux personnel

(BLD HR)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie de sécurité de l'information et protection de la vie privée au sein de la sécurité sociale. Ce document est destiné aux responsables et aux sous-traitants de l'information, 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).

Ce document décrit la politique relative aux aspects liés au personnel en ce qui concerne la sécurité de l'information et la protection de la vie privée.

2. Aspects liés aux personnel

Toute organisation souscrit la politique relative à la sécurité de l'information et à la protection de la vie privée pour l'ensemble des informations et systèmes d'information relevant de la responsabilité de l'organisation :

Préalablement au contrat de travail : faire en sorte que les travailleurs, le personnel auquel il est fait appel et les utilisateurs externes comprennent leurs responsabilités, soient compétents pour les rôles pour lesquels leur engagement est envisagé et faire en sorte de limiter le risque de vol, de fraude ou d'abus des facilités.

- Vérifier le milieu familial et socioculturel des candidats aux fonctions qui impliquent un risque majeur pour la sécurité de l'information; cette vérification peut 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 : faire en sorte que les travailleurs, le personnel auquel il est fait appel et les utilisateurs externes soient conscients des menaces et des dangers pour la sécurité de l'information et de leur responsabilité. Ils doivent être équipés pour soutenir la politique de sécurité de l'organisation dans les activités quotidiennes et limiter le risque d'erreur humaine.

- 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 protection de la vie privée, conformément aux directives, 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 complémentaire relative aux directives, 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 collaborateurs qui exercent une fonction qui implique 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-respect telles que prévues dans la législation.

Cessation ou modification du contrat de travail: faire en sorte que les intérêts de l'organisation soient préservés lorsque des travailleurs, du personnel auquel il est fait appel et des utilisateurs externes quittent l'organisation ou modifient leur 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 utilisateurs externes et doivent être rendues obligatoires.

Par ailleurs, toute organisation doit :

1. 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. Le service de sécurité de l'information a une mission de conseil, de stimulation, de documentation et de contrôle (au sens de l'AR de 1993). En vue de la sécurité des données sociales traitées par son organisation et en vue de la protection de la vie privée des personnes auxquelles ces données sociales ont trait, le conseiller en sécurité est chargé :
    a. de fournir des avis qualifiés à la personne chargée de la gestion journalière.
    b. d'exécuter des missions qui lui sont confiées par la personne chargée de la gestion journalière.
2. 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'organisation.
3. disposer d'un plan de sécurité approuvé par le responsable de la gestion journalière (ou équivalent) de l'organisation concernée.
4. 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.
5. 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.
6. planifier la communication d'informations au conseiller en sécurité de sorte que celui-ci dispose des données nécessaires pour l'exécution de ses missions, ainsi que pour l'organisation de la concertation entre les différentes parties concernées[1] afin d'associer davantage le conseiller en sécurité aux travaux de l'organisation.

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.

Toute organisation d'un réseau secondaire est tenue d'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.

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.

1 Les parties visées dans cette politique 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.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2003		V2003	Première version	10/09/2003	1/10/2003
2004		V2004	Deuxième version	11/02/2004	1/12/2004
2017		V2017	Intégration UE GDPR	7/03/2017	7/03/2017

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 p.

Ci-dessous figurent les références aux sites web qui ont service de source d'inspiration pour le présent document:

- https://www.iso.org/fr/isoiec-27001-information-security.html
- https://www.iso.org/fr/standard/54534.html
- https://www.iso.org/fr/standard/54533.html
- http://www.isaca.org/cobit
- https://www.ksz-bcss.fgov.be/fr
- http://www.ccb.belgium.be/fr/work
- https://www.safeonweb.be/fr
- https://www.safeinternetbanking.be/fr
- https://www.cybersimpel.be/fr

Annexe C: Directives relatives aux aspects de la sécurité de l'information et de la protection de la vie privée liés au personnel

Préalablement au contrat de travail

Screening

- Les responsabilités à l'égard de la sécurité de l'information doivent être définies, préalablement au contrat de travail, dans des descriptions de fonction appropriées et dans les conditions de travail.
- Les candidats à une fonction qui implique un risque important pour la sécurité de l'information, en particulier les fonctions de confiance et les fonctions de sécurité, peuvent faire l'objet d'un screening.
- Les fonctions qui impliquent un risque important pour la sécurité de l'information doivent être identifiées et documentées par l'organisation.
- Des procédures doivent décrire sur base de quels critères les vérifications peuvent être effectuées, qui peut les effectuer, quand et comment.

Conditions de travail

- Le personnel auquel il est fait appel et les utilisateurs externes qui emploient du matériel ICT doivent signer une convention relative à leurs rôles et responsabilités par rapport à la sécurité de l'information.
- Le cahier des charges d'un marché public doit contenir les principes fondamentaux à respecter par l'adjudicataire et son personnel et à appliquer lors de l'exécution du marché. Les principes fondamentaux de la sécurité de l'information et de la protection de la vie privée seront complétés et précisés davantage au moyen de directives spécifiques pendant l'exécution du marché. Ces directives ne peuvent aucunement porter atteinte aux principes fondamentaux.
- Le personnel qui est mis à la disposition de l'organisation par un fournisseur dans le cadre d'un marché public est tenu de respecter les conditions définies dans le cahier des charges ainsi que les directives spécifiques communiquées au cours de l'exécution du marché.
- Les rôles et responsabilités en matière de sécurité de l'information et de protection de la vie privée doivent être communiqués aux candidats à un emploi dès le processus d'engagement.

Pendant le contrat de travail

Responsabilité de la direction

- Les travailleurs, le personnel auquel il est fait appel et les utilisateurs externes doivent être informés de manière adéquate de leurs rôles et responsabilités et doivent recevoir les directives nécessaires, avant de pouvoir accéder à des informations confidentielles ou à des systèmes d'information de l'organisation.

Sensibilisation, formation et coaching en matière de sécurité de l'information et de protection de la vie privée.

- Un programme de sensibilisation en matière de sécurité de l'information et de protection de la vie privée doit être élaboré de manière conforme à la politique et aux procédures de sécurité de l'information et de protection de la vie privée en vigueur.
- Un programme de sensibilisation doit être composé de diverses initiatives de sensibilisation telles que des sessions d'information, des lettres d'information, des affiches, etc. et doit être régulièrement actualisé et organisé.
- La formation en matière de sécurité de l'information et de protection de la vie privée doit être régulièrement organisée, tant à l'attention des nouveaux collaborateurs qu'à l'attention des travailleurs qui changent de fonction ou de rôle au sein de l'organisation.

Actualisation du screening

- Les candidats à une fonction qui implique un risque important pour la sécurité de l'information et la protection de la vie privée, en particulier les fonctions de confiance et les fonctions de sécurité, peuvent régulièrement faire l'objet d'un screening.

Mesures disciplinaires

- La constatation du fait que la politique et les procédures y afférentes - dont le personnel a été informé - ne sont pas respectées peut donner lieu à des sanctions et même à des poursuites judiciaires.
- Les mesures disciplinaires pour les travailleurs de l'organisation doivent être conformes aux sanctions internes prévues par la loi.
- Les sanctions pour le personnel auquel il est fait appel et les contractants, autres que celles prévues dans la législation générale ou dans la législation et réglementation relatives aux marchés publics, doivent être mentionnées dans le cahier des charges.

Cessation ou modification du contrat de travail

- Les responsabilités sur le plan de la sécurité de l'information et de la protection de la vie privée qui doivent encore être assumées après la fin du contrat de travail doivent préalablement faire l'objet de clauses spéciales ou de contrats de travail.
- La personne responsable au sein de l'organisation du contrôle et du suivi du personnel auquel il est fait appel et des utilisateurs externes doit appliquer les directives précitées au personnel auquel il est fait appel et aux utilisateurs externes.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	**Oui**
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	
Relations avec les fournisseurs	
Gestion des incidents de sécurité	
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	

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