Politique de sécurité de l'information et vie privée

Code de bonne conduite pour les gestionnaires d'information

(BLD ETHICS)

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. 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).

A l'heure actuelle, personne ne doute du fait que la technologie de l'information et de la communication (TIC) joue un rôle important dans la vie économique. Le fonctionnement correct des systèmes d'information, en ce compris du matériel et des logiciels, est d'une importance cruciale pour les pouvoirs publics, les organisations et les citoyens qui sont fortement dépendants de ces systèmes et par conséquent de leurs gestionnaires d'information[1].

Avant de préciser les rôles et responsabilités des gestionnaires d'information, il paraît utile de rappeler les missions du conseiller en sécurité de l'information au sein du réseau de la sécurité sociale. En effet, le conseiller en sécurité de l'information est tenu de faire respecter les lois relatives à la protection de la vie privée. Il a aussi un rôle de conseil, de stimulation, de documentation, de contrôle et de promotion en matière de respect des règles de sécurité de l'information imposées par une disposition réglementaire ou légale ou en vertu d'une telle disposition. Il doit aussi veiller à ce que tous les collaborateurs adoptent une attitude visant à encourager la sécurité. Le conseiller en sécurité de l'information est à cet égard un partenaire privilégié des gestionnaires d'information. Le conseiller en sécurité de l'information est tenu de respecter un code éthique de bonne conduite.

Le gestionnaire d'information est toute personne qui, dans le cadre de ses responsabilités en matière de système ICT, dispose de droits d'accès plus larges que la simple utilisation fonctionnelle des informations (« superusers » ou « powerusers »). Il s'agit notamment des gestionnaires systèmes, des administrateurs de banques de données (DBA), des conseillers en sécurité de l'information (CISO), des délégués à la protection des données (DPO), des développeurs et des gestionnaires de logiciels, des gestionnaires réseaux, des consultants, des fournisseurs de services IT externes[2] et des sous-traitants.

Le présent code de bonne conduite n'a pas l'ambition de décrire la tâche précise du gestionnaire d'information ou d'être un manuel technique pour les gestionnaires d'information. Ceci a en effet déjà été réalisé dans d'autres documents telles les lignes politiques, les descriptions de fonction ou les règlements de travail. Le présent code de bonne conduite n'offre pas de solution concrète pour tout problème éthique ou politique auquel un gestionnaire d'information est confronté lors de l'exécution de sa fonction.

Le présent code de bonne conduite entend sensibiliser les gestionnaires d'information à l'importance d'exercer leurs compétences de manière éthique. En effet, l'intégrité d'un gestionnaire d'information fait intégralement partie de son professionnalisme. Les gestionnaires d'information peuvent utiliser ce code de bonne conduite comme directive pour les travaux quotidiens. Le gestionnaire d'information peut, par ailleurs, considérer ce code de bonne conduite comme une invitation permanente pour évaluer l'ensemble des actes professionnels au niveau éthique et les adapter si nécessaire. Pour tous les autres collaborateurs de l'organisation, il est important de savoir que l'exercice des compétences de gestionnaire d'information est soumis à des règles. Pour la direction, il est utile de préciser comment le gestionnaire d'information doit utiliser ses compétences dans l'intérêt de l'organisation.

Ce code de bonne conduite pour les gestionnaires d'information part de trois notions de base, à savoir l'intégrité, la protection de l'information et l'obligation d'information et de documentation. En ce qui concerne l'intégrité, il s'agit tant de l'intégrité éthique du gestionnaire d'information que de l'intégrité des systèmes d'informations. La protection des informations a trait tant à la protection de la vie privée qu'au traitement de données confidentielles. L'obligation

[1] En anglais, on utilise souvent le terme « data custodian » qui ne peut être confondu avec le terme « data steward ». Les « data stewards » sont responsables pour le contenu des données, le contexte et les règles d'entreprise y afférentes. Les « data custodians » sont responsables pour la conservation, le transport, l'enregistrement des données et l'exécution des règles professionnelles. En d'autres termes, les « data stewards » sont responsables pour ce qui est enregistré dans un champ de données, alors que les « data custodians » sont responsables pour l'environnement technique et la structure de la base de données.

[2] Des exemples de fournisseurs de services IT externes sont les fournisseurs de services internet (ISP), les fournisseurs de services applicatifs (ASP), les fournisseurs de services cloud (CSP) ou les cloud service brokers (CSB).

d'information/de documentation concerne l'information de collaborateurs et la documentation de systèmes d'information.

Le présent document décrit les directives contenant les règles à respecter par les gestionnaires d'information qui travaillent dans les institutions faisant partie du réseau de la sécurité sociale.

2. Code de bonne conduite

Toute organisation souscrit les directives 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:

1. La direction de l'organisation doit mettre au point, valider, communiquer et tenir à jour un code de bonne conduite pour les gestionnaires d'information relatif à l'intégrité, à la protection de l'information et à l'obligation d'informations/de documentation.
2. La direction de l'organisation se réserve le droit de contrôler le code de bonne conduite.
3. L'organisation doit disposer d'une procédure de notification formelle et d'un processus disciplinaire pour les collaborateurs ayant enfreint le code de bonne conduite.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2005		V2005	Première version	29/06/2005	01/07/2005
2005		V2005	Deuxième version	12/09/2005	01/10/2005
2017		V2017	Intégration UE GDPR	07/03/2017	07/03/2017

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.
- ADM, "Gedragscode voor informatiebeheerders", septembre 2010, 7 p.

Ci-dessous figurent les références aux sites web qui ont servi 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
- http://www.isaca.org/certification/code-of-professional-ethics/pages/default.aspx
- https://www.sans.org/security-resources/ethics
- https://en.wikibooks.org/wiki/Ethics_for_IT_Professionals/Professional_Code_of_Ethics
- http://ethics-wg.org/framework.html
- https://digital-forensics.sans.org/certification/ethics
- https://www.ksz-bcss.fgov.be/fr
- http://www.ccb.belgium.be/fr

Annexe C: Code de bonne conduite

I. L'intégrité éthique du gestionnaire d'information

I.1. Le gestionnaire d'information adopte une attitude objective et impartiale pendant l'exercice de sa fonction.

Explication: la présente directive générale décrit l'attitude du gestionnaire d'information. Le gestionnaire d'information assume cette fonction d'une manière critique et réfléchie. Il essaie de tenir compte autant que possible des différents intérêts en jeu et prend ses décisions sur la base d'une évaluation rationnelle de toutes les informations pertinentes disponibles.

I.2. Le gestionnaire d'information essaie d'éviter des conflits d'intérêts personnels (ou la perception de ces conflits). Toutefois, si ceux-ci se manifestent malgré tout, il en informera directement ses supérieurs et demandera une décision formelle à ce sujet.

Explication: il s'agit d'intérêts personnels qui sont incompatibles avec l'intérêt de l'organisation, par exemple sécuriser la position au sein de l'organisation par des pratiques et des comportements non corrects. Le gestionnaire d'information ne peut pas accepter de cadeaux, dons ou invitations de tiers ou de consultants externes ou de collaborateurs temporaires sans la communication explicite préalable à la personne chargée de la gestion journalière de l'organisation et sans son approbation.

I.3. Le gestionnaire d'information met ses compétences au service de l'organisation et des collaborateurs des systèmes d'information, et ce de manière appropriée.

Explication: un gestionnaire d'information dispose de connaissances et d'une expertise très précieuses, et doit veiller à ce que ces connaissances et cette expertise soient utilisées, dans des conditions adéquates, dans l'intérêt de l'organisation (ou pour atteindre les objectifs de l'organisation).

I.4. Le gestionnaire d'information essaie de collaborer avec l'ensemble des collaborateurs de l'organisation, dans une entente aussi optimale que possible.

Explication: le gestionnaire d'information ne peut devenir un étranger pour son organisation ou adopter une telle attitude au détriment des intérêts ou objectifs de l'organisation. Les consultants externes et les collaborateurs temporaires sont également considérés comme employés au sein de l'organisation.

I.5. Le gestionnaire d'information présentera ses compétences techniques en toute honnêteté et fera appel à une aide professionnelle (technique) supplémentaire si nécessaire.

I.6. Le gestionnaire d'information reçoit les moyens et fournit des efforts suffisants pour rester au courant des évolutions dans son domaine.

I.7. Le gestionnaire d'information collabore et entretient des contacts respectueux avec l'ensemble des collaborateurs (internes et externes).

I.8. Le gestionnaire d'information collaborera avec les autorités (de contrôle).

II. L'intégrité et la disponibilité des informations

II.1. Le gestionnaire d'information veille au fonctionnement correct du système et pose les actes nécessaires permettant de garantir l'intégrité et la disponibilité du système d'information.

Explication: le gestionnaire d'information ne pose aucun acte contraire à la garantie du bon fonctionnement du système d'information de l'organisation.

II.2. Le gestionnaire d'information veille à ce que les actes n'entraînent pas la perte, l'indisponibilité ou la destruction des données ou des applications.

II.3. Étant donné que certains actes de collaborateurs sont susceptibles de porter atteinte à l'intégrité ou de compromettre la disponibilité du système ou du réseau informatique ou des données, le gestionnaire d'information doit, dans le cadre de ses responsabilités, veiller au respect de la politique qui est d'application dans l'organisation et doit, si nécessaire, informer ses supérieurs hiérarchiques. S'il constate que certains actes ne tombent pas sous le champ d'application des normes minimales existantes, il en informe le conseiller en sécurité de l'information. Le conseiller en sécurité de l'information prendra les mesures nécessaires dans l'intérêt de l'organisation.

II.4. Le gestionnaire d'information veille à ce que l'accès au système d'information soit garanti aux personnes qui ont besoin de cet accès dans le cadre de leur fonction et que cet accès reste limité à ces personnes.

III. Protection des informations

Respect du règlement[3] relatif à la vie privée et à la protection des données sensibles

III.1. Le gestionnaire d'information est conscient du fait qu'il a accès à de grandes quantités de données à caractère personnel et de données sensibles auxquelles s'appliquent les dispositions relatives à la protection de la vie privée et des données à caractère personnel.

Explication: par « donnée à caractère personnel », on entend toute information concernant une personne physique identifiée ou identifiable (« la personne concernée »); est réputée identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel un nom, un numéro d'identification, des données de localisation, à un identifiant en ligne ou à un ou plusieurs éléments propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

III.2. Le gestionnaire d'information est conscient du fait que les données à caractère personnel et les données sensibles doivent être protégées.

III.3. Le gestionnaire d'information attire l'attention sur les risques propres à son domaine, insiste auprès de sa direction pour obtenir des instructions adéquates relatives à ces risques et met en œuvre des mesures organisationnelles, communicatives, procédurales et techniques, ce qui permet de protéger les données à caractère personnel et les données sensibles contre tout traitement de données à caractère personnel non autorisé. Le gestionnaire d'information tient compte, outre des risques liés au traitement, de la nature, de l'ampleur, du contexte et des finalités du traitement.

Explication: afin de déterminer ce que sont des instructions « adéquates », il y a lieu de tenir compte de la technique en la matière et du coût d'application des mesures de contrôle, d'une part, et de la nature des informations à protéger et des risques potentiels, d'autre part.

III.4. Le gestionnaire d'information veille aussi à ce que les tiers et les collaborateurs externes respectent les dispositions relatives à la protection des données à caractère personnel et des données sensibles.

Explication: par exemple, en cas de maintenance ou de réparation de systèmes d'information par des tiers ou des collaborateurs externes, ceux-ci doivent aussi être au courant des obligations pertinentes en matière de protection des données à caractère personnel et des données sensibles.

Contrôle de la communication et de l'accès en ligne aux fichiers

III.5. Le gestionnaire d'information peut contrôler la communication et les accès en ligne aux fichiers dans le cadre de ses compétences et moyennant le respect des dispositions légales et réglementaires.

Explication: En principe, le contrôle des données de communication électroniques en ligne ne peut entraîner une ingérence dans la vie privée du collaborateur. Si le contrôle entraîne tout de même une ingérence dans la vie privée du collaborateur, cette ingérence doit être limitée au strict minimum. Les contrôles secrets sont interdits. Par ailleurs, le contrôle est uniquement possible pour: 1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui; 2° la protection des intérêts économiques, commerciaux et financiers de l'organisation auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires; 3° 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; 4° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'organisation.

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

Données confidentielles

III.6. Le gestionnaire d'information part du principe que l'ensemble des informations de l'organisation sont confidentielles et qu'elles doivent donc être traitées en tant que telles, tant par lui-même que l'ensemble des collaborateurs de l'organisation.

Explication: outre des données à caractère personnel (dont des données sociales et des données médicales), il s'agit aussi des secrets professionnels, du savoir-faire et d'autres informations sensibles. Aucun gestionnaire d'informations ne peut abuser de ces informations.

IV. Obligation d'information et de documentation

IV.1 Le gestionnaire d'information informe régulièrement et clairement tous les collaborateurs concernés sur les responsabilités en cas d'usage autorisé des systèmes d'information via une sensibilisation, une formation et des évaluations (ou des audits d'évaluation).

IV.2. À l'occasion d'une intervention, le gestionnaire d'information explique ses actes de manière compréhensible et dans les délais utiles, de sorte que le(s) collaborateur(s) soit(en)t suffisamment informé(s) sur les conséquences sur les systèmes d'information (ou l'usage des systèmes d'information).

Explication: il s'agit d'interventions du gestionnaire d'informations, par exemple dans le cadre de l'adaptation d'un système.

IV.3. Le gestionnaire d'information veille à ce qu'une documentation actualisée soit disponible à tout moment. Cette documentation doit décrire le système d'information (tel que le développement, les logiciels et le matériel, l'infrastructure) de la sorte que toute personne concernée puisse se faire une image précise et complète de la situation. L'objectif est de garantir une gestion continue du système d'information. L'analyse d'impact relative à la protection des données en fait partie intégrante.

Explication: si le gestionnaire d'information n'est plus en mesure d'exercer sa fonction pour l'une ou l'autre raison, un autre gestionnaire d'information doit pouvoir continuer à gérer efficacement le système d'information. Afin de faciliter le transfert de connaissances, un inventaire complet et précis des systèmes d'information constitue une base.

IV.4. Le gestionnaire d'information peut poser des questions à d'autres gestionnaires d'informations de l'organisation ou discuter de problèmes avec ces derniers ou peut si nécessaire aussi les examiner en toute confidentialité avec le service Sécurité de l'information de la BCSS.

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	**Oui**

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