ISMS

(Information Security Management System)

Politique de sécurité de l'information

(Information Security Policy)

2008

Version control – please always check if you're using the latest version Doc. Ref. : isms.001.ISP				
Release	Status	Date	Written by	Approved by
FR_1.0	Proposition pour les institutions de sécurité sociale	25/06/2008	Johan Costrop	Groupe de Travail Sécurité de l'information

Remarque : Ce document intègre les remarques d'un groupe de travail auquel ont participé madame Minnaert (INASTI) et messieurs Bochart (BCSS), Bouamor (CIMIRe), Costrop (Smals), De Ronne (ONVA), De Vuyst (BCSS), Petit (FMP), Quewet (SPP SP), Symons (ONEm), Van Cutsem (ONSS APL), Van den Heuvel (BCSS), Vandergoten (INAMI) et Vertongen (ONSS).

Table des matières

1 Définition de la sécurité de l'information

L'information est un moyen de production qui, à l'instar d'autres moyens de production importants, représente une valeur considérable et qui doit donc être protégé de manière appropriée.

La sécurité de l'information protège l'information d'une multitude de menaces. Les institutions, leurs systèmes d'information et réseaux sont de plus en plus confrontés à un nombre croissant de risques divers en provenance de sources diverses. Songeons par exemple aux virus informatiques, au piratage informatique, au refus de service informatique (*denial of service*), à la fraude informatique, mais également à la perte, au vol (p.ex. d'un ordinateur portable), à la divulgation de données confidentielles, au risque d'incendie, …

Le maintien et l'amélioration de la sécurité de l'information peut s'avérer d'une importance fondamentale pour assurer la continuité du fonctionnement de l'institution, le respect de la loi mais également pour l'image de l'institution.

De manière générale, la sécurité de l'information se caractérise par la garantie de la confidentialité (confidentiality), de l'intégrité (integrity) et de la disponibilité (availability) de l'information. A titre complémentaire, la sécurité de l'information proposera des moyens permettant de réfuter des informations falsifiées et de rendre impossible la réfutation d'informations légitimes.

Dans le domaine spécifique de la sécurité sociale, la sécurité de l'information est définie comme la prévention et la réparation efficiente des dommages aux données sociales et des violations illégitimes de la vie privée des intéressés (Cfr. arrêté royal de 1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale).

2 Objectif de la sécurité de l'information auprès de l'institution

2.1 Objectif

La sécurité de l'information auprès de l'institution vise la pérennité et le bon fonctionnement des activités de l'institution, elle est en premier lieu axée sur la prévention de dommages, en vue de la réalisation des objectifs formulés dans sa mission.

De manière plus générale, elle vise en outre à éviter tout dommage pouvant affecter le bon fonctionnement des systèmes d'information de la sécurité sociale d'une part et la vie privée des intéressés d'autre part.

En effet, l'informatisation des institutions de sécurité sociale et leur collaboration accrue donnent lieu à des améliorations considérables sur le plan de l'efficacité et de l'efficience, mais entraînent en même temps de nouveaux risques. Les différentes institutions de sécurité sociale ne sont plus des entités isolées qui traitent des informations, mais elles font partie d'un groupe cohérent. Les liens de collaboration accrus augmentent considérablement le risque et l'ampleur des dommages collatéraux. C'est pourquoi la vision en matière de sécurité de l'information et de protection de la vie privée est définie collectivement.

Une perturbation importante de la sécurité de l'information auprès de l'institution aura un impact négatif sur le fonctionnement de la sécurité sociale.

2.2 Obligations légales et normes minimales de sécurité

Dans le cadre de la sécurité de l'information de la sécurité sociale, plusieurs obligations légales et normes minimales doivent également être respectées.

3 Approche générale en matière de sécurité de l'information auprès de l'institution

3.1 Cadre général

La sécurité de l'information pouvant être atteinte à l'aide de moyens techniques est trop limitée et doit être soutenue par une gestion et des procédures adéquates. Pour déterminer les mesures de gestion à mettre en place, un planning minutieux et une analyse méticuleuse sont requis. Ces mesures doivent en tout cas porter entre autres sur la gestion, les règles de conduite, les procédures, les structures organisationnelles, le développement, la maintenance, la continuité, les contrôles, etc.

La sécurité doit être à l'initiative, au support et à la responsabilité du management. La participation de l'ensemble des collaborateurs de l'institution est cruciale. La contribution des fournisseurs, des clients ou d'autres partenaires externes est également importante.

Par ailleurs, il faut essayer de trouver un bon équilibre entre des mesures de prévention d'une part (prévention d'incidents de sécurité) et des mesures correctives d'autre part (limiter les conséquences négatives d'incidents).

3.2 Approche basée sur la série de normes ISO 2700X

Au sein de la sécurité sociale, l'approche en matière de sécurité de l'information est déterminée de façon collective. De façon générale, la sécurité de l'information y est basée sur la série de normes internationales ISO 2700X.

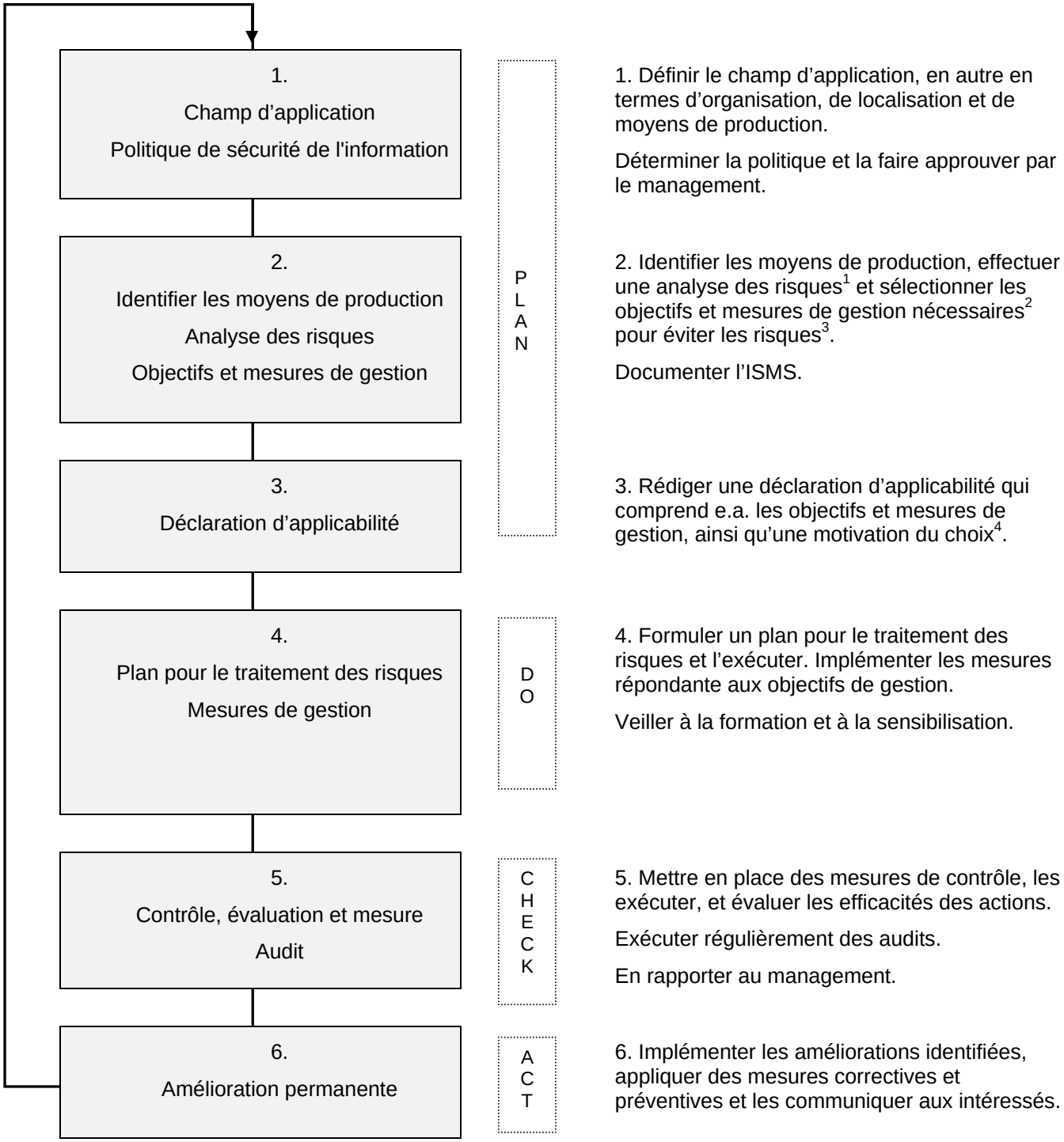
La norme ISO 27001 offre un modèle général (un cadre) pour la détermination, la mise en œuvre, l'exécution, le contrôle, l'évaluation, le maintien et l'amélioration d'un système de gestion documenté en matière de sécurité de l'information (ISMS - information security management system).

ISO 27002 contient un aperçu détaillé des mesures de gestion possibles.

L'ISMS permet de choisir les mesures de gestion appropriées. A cet égard, il est également tenu compte des besoins spécifiques, des exigences en matière de sécurité, de la taille et de la structure de l'institution. Au sein des institutions de sécurité sociale, les mesures de gestion sont par exemple complétées par des mesures spécifiques pertinentes dans le domaine de la sécurité sociale et de la protection de la vie privée.

Cette approche, structurée selon le modèle "*Plan-Do-Check-Act*", met l'accent sur la nécessité de comprendre les exigences de l'institution en matière de sécurité de l'information et de définir des policies et des objectifs en la matière. Elle permet de mettre en œuvre des mesures de gestion, de les contrôler et d'évaluer leur efficacité. Un processus d'amélioration permanente est par ailleurs mis en œuvre.

De façon schématique, cette approche se présente comme suit:



[1] Quoique souhaitable, il n'est pas toujours nécessaire et opportun d'effectuer une analyse des risques détaillée, il suffit alors d'examiner uniquement les lignes de base. Dans ce cas, les priorités sont au minimum basées sur : *1*. les risques les plus importants; *2*. les obligations légales et contractuelles; *3*. les obligations internes de l'institution.

[2] Ces mesures sont basées sur la norme ISO 27002, complétée par des mesures spécifiques pertinentes pour le secteur de la sécurité sociale et la problématique de la protection de la vie privée.

[3] Les coûts des mesures de sécurité doivent être en propotionnelle tant avec la valeur du moyen de production qu'avec le dommage qui peut résulter d'un incident.

[4] La motivation de la sélection des objectifs et mesures de gestion est e.a. basée sur la concertation au sein du groupe de travail Sécurité de l'information du Comité général de coordination.

4 Politique de sécurité de l'information

Introduction

Dans le cadre d'un ISMS, la "Politique de sécurité de l'information" est un document de base important. Le management de l'institution indique les objectifs à poursuivre en matière de sécurité de l'information.

Les paragraphes suivants présentent, sans entrer dans les détails, les principales mesures de gestion cadrant avec l'ISMS de l'institution. Sur base des thèmes mentionnés ici, des documents de politique spécifiques (« policies ») peuvent être rédigés.

Ce document sera revu périodiquement, entre autres après l'évaluation de la politique à l'occasion d'incidents de sécurité importants, de nouvelles vulnérabilités ou de modifications dans l'infrastructure organisationnelle ou technique (le responsable du document est le chef du service de sécurité de l'information).

Champ d'application

La "Politique de sécurité de l'information" s'applique à l'ensemble du personnel tant interne qu'externe et ce y compris le personnel mis à disposition, et tant à durée déterminée que indéterminée (ex. sous-traitants, consultants, fournisseurs,...). Elle s'applique également à tous les systèmes d'information développés, opérationnels et à développer (y compris l'information qu'ils contiennent) de tous les sites de l'institution concernée.

4.1 Organisation de la sécurité de l'information

4.1.1 L'organisation de la sécurité de l'information a pour objectif de gérer la protection de l'information au sein de l'institution.

4.1.2 Cette organisation de la sécurité s'inscrit dans le cadre des structures définies dans la législation en matière de sécurité de l'information dans les institutions de sécurité sociale. Le service de sécurité de l'information joue un rôle clé à cet égard.

4.1.3 La "Plateforme de décision pour la sécurité de l'information" oriente la politique de sécurité : la révision de la politique, l'ajustement des mesures de sécurité, l'établissement de plans de sécurité, la détermination des responsabilités et la surveillance de l'évolution des menaces et des incidents. Cette platforme est supportée activement par le management. Ce dernier lui donne la direction et montre son engagement envers elle.

4.1.4 Les rôles et responsabilités en matière de protection de l'information y sont définis.

4.1.5 Les aspects organisationnels de la collaboration avec des tiers (ex. sous-traitance de tâches) constituent également un point d'attention. Les aspects de sécurité de la collaboration sont fixés par contrat.

4.1.6 Dans le cadre de la protection physique, le service de sécurité de l'information et le "service interne pour la prévention et la protection au travail" sont appelés à collaborer étroitement.

4.2 Gestion des ressources[5]

4.2.1 La gestion des ressources a pour objet le maintien d'une protection adéquate de ces ressources.

4.2.2 Les ressources doivent être inventoriées.

4.2.3 Des données confidentielles sont traitées dans le contexte de la sécurité sociale. Le traitement de ces données est soumis à une législation spécifique, notamment en matière de protection de la vie privée, en ce y compris la législation en matière de données médicales.

4.2.4 Les données sont traitées conformément à leur classification.

4.3 Sécurité liée aux collaborateurs tant interne, qu'externe

4.3.1 Cette politique vise à mettre à profit l'expérience des collaborateurs et à maintenir à niveau leurs connaissances dans le but de promouvoir la sécurité de l'information.

4.3.2 Les collaborateurs doivent être conscients des menaces pesant sur la sécurité de l'information et de l'importance qu'elle revêt. Ils doivent disposer des moyens, des connaissances et des compétences appropriés à cette fin.

4.3.3 Il est tenu compte du fait que les collaborateurs de l'institution travaillent dans divers endroits (bâtiments, chantiers, …). Des mesures de sécurité spécifiques peuvent être mises en place dans ces lieux.

4.3.4 La politique du personnel y contribue, par exemple en intégrant des aspects de sécurité dans les descriptions de fonction, en prévoyant des déclarations de respect de la confidentialité, en mentionnant dans le règlement de travail ou le contrat de travail la responsabilité du travailleur en matière de sécurité de l'information, ou en rédigeant un code de bonne conduite .

4.3.5 Pour les fonctions de management ou les fonctions impliquant un accès à des données confidentielles, le candidat est sélectionné sur la base de son curriculum vitae et de ses antécédents judiciaires, selon les règles applicables au sein de l'institution.

4.3.6 Tout collaborateur est tenu de signaler les risques et les incidents de sécurité.

4.3.7 L'attention des collaborateurs est attirée sur leur responsabilité en ce qui concerne le maintien d'une protection efficace de l'accès, notamment sur le plan de l'utilisation de mots de passe et la sécurité du matériel des utilisateurs.

4.3.8 Un point d'attention particulier, surtout pour les collaborateurs du helpdesk (ex. centre de contact), concerne les techniques de "social engineering" qui consistent à obtenir des informations essentielles (ex. mots de passe) par tromperie.

4.3.9 L'attention des collaborateurs est attirée sur les risques de sécurité qu'entraînent les systèmes électroniques (ex. ordinateurs, ordinateurs portables, téléphones, téléphones portables, e-mail, courrier, messagerie vocale, services postaux, fax,...) : ces systèmes impliquent un risque pour la confidentialité des données d'exploitation.

[5] Dans le présent contexte, les ressources sont notamment le matériel, les logiciels et les données.

4.3.10 L'utilisation de ressources à des fins privées doit être limitée à un strict minimum. Exemples:

- L'accès à Internet ne peut pas être employé à des activités susceptibles de nuire à l'institution (p.ex. réputation, bon fonctionnement, infraction à la loi, …).
- L'envoi d'e-mails personnels pendant les heures de travail doit se limiter à un strict minimum.

4.3.11 L'attention des collaborateurs est attirée sur leur responsabilité quant à l'utilisation des ressources de l'entreprise :

A titre d'exemple, nous pouvons citer les risques suivants :

- compromettre l'organisation par l'envoi d'e-mails inconvenants, participation à des forums internet inconvenants, visites de sites internet inappropriés.
- vigilance lors de l'ouverture d'e-mails et de pièces jointes.

4.3.12 Sur les appareils directement connectés à l'infrastructure de l'institution (p.ex. PC), seuls les services compétents désignés par l'institution peuvent installer des logiciels et régler les configurations.

4.3.13 Lorsqu'un collaborateur quitte le service ou change de fonction, les droits d'accès et les autorisations sont adaptées au plus vite et le matériel physique est éventuellement récupéré.

4.3.14 Le non-respect de la politique de sécurité et des procédures de sécurité de l'organisation est traité suivant un processus formel.

4.4 Sécurité physique et protection de l'environnement

4.4.1 Cette politique a pour but

- de prévenir l'accès physique non autorisé ou inutile à l'information et aux systèmes d'information afin de limiter la prise de connaissance non autorisée, l'altération ou le vol d'informations ;
- de prévenir les dommages aux systèmes d'information ou leur perturbation.

4.4.2 Il faut tenir compte de la localisation des bâtiments qui hébergent l'institution de sécurité sociale (bâtiments dispersés, intégration de services dans d'autres bâtiments, …), ce qui accroît également le risque d'accès non autorisé.

4.5 Gestion opérationnelle

4.5.1 Cette politique vise à garantir une manipulation et un fonctionnement corrects et sûrs des équipements des systèmes d'informations.

4.5.2 Il faut tenir compte du fait que le risque d'attaques sur le système augmente au même rythme que la visibilité des applications électroniques de la sécurité sociale.

4.5.3 Les responsabilités et les procédures sont définies en ce qui concerne :

- la gestion et la manipulation de tous les équipements des systèmes d'informations.
- le contrôle de toutes les modifications aux appareils, logiciels et procédures,
- le traitement des incidents.

4.5.4 Lorsqu'il y a un risque de sécurité, une séparation des fonctions est opérée afin de limiter le risque de conflits d'intérêts.

4.5.5 Les dispositifs pour le développement, les tests / l'acceptation et la production sont séparés.

4.5.6 Avant que les dispositifs des systèmes d'informations entrent en phase opérationnelle, il est vérifié que toutes les exigences de sécurité (fonctionnalité, sécurité, …) ont été implémentées et testées.

4.5.7 Lorsque des activités ICT sont confiées en sous-traitance à une entreprise externe, les risques de sécurité font l'objet d'une attention spéciale. Les aspects de sécurité sont réglés dans le contrat.

4.5.8 L'accès des gestionnaires d'information[6] aux systèmes informatiques doit être limité au moyen d'une identification, authentification et autorisation.

4.5.9 Une gestion des capacités et des procédures d'acceptation appropriées pour les systèmes ICT (pas seulement pour les systèmes ICT neuf, mais également pour tout systèmes modifiés par mise à jours, upgrade, …) limite aux maximum le risque de perturbation.

4.5.10 Afin d'assurer la protection de l'intégrité des logiciels et des informations, des mesures sont prises pour éviter et détecter des logiciels nuisibles et pour en limiter autant que possible les conséquences éventuelles.

De même, les signalements de nouvelles menaces par des instances compétentes sont suivis et les mesures nécessaires sont prises (e.a. patches software).

4.5.11 Selon les consignes de sécurité concernées, des sauvegardes des informations essentielles et des logiciels doivent régulièrement être prises pour maintenir l'intégrité et la disponibilité des services. Ces sauvegardes doivent régulièrement être testées.

4.5.12 Le maintien de la sécurité des informations au sein des réseaux (comme l'extranet de la sécurité sociale) et la protection de l'infrastructure sous-jacente font l'objet d'une attention spéciale. Des mesures maximales sont prises lors du transport de données sensibles via des réseaux publics (ex. Internet).

4.5.13 Les moyens de stockage sont protégés contre la détérioration, le vol et l'accès non autorisé.

4.5.14 Dans le respect des dispositions légales en matière de conservation et d'utilisation des données archivées, toute évolution de l'infrastructure informatique et du système d'information requiert un contrôle de l'adéquation entre les données archivées, les supports de stockage utilisés et les applications nécessaires à leur exploitation.

4.5.15 Des mesures sont prises pour éviter la perte, la modification ou le mauvais usage d'informations échangées avec d'autres organisations (en particulier les institutions de sécurité sociale).

[6] Le gestionnaire de l'information est toute personne qui, dans le cadre de ses responsabilités en ce qui concerne un système ICT, dispose de droits d'accès plus larges que la simple utilisation fonctionnelle des données. Il s'agit entre autres de développeurs, de gestionnaires de systèmes, de gestionnaires de données, de développeurs et gestionnaires de logiciels, de gestionnaires de réseaux, de consultants et de sous-traitants.

4.5.16 La protection de l'intégrité de l'information sur des systèmes accessibles au grand public (tels que des serveurs web) requiert une attention particulière pour éviter des modifications non autorisées susceptibles de nuire à l'institution ou à l'une des organisations de la sécurité sociale[7].

4.5.17 Si des supports et/ou des informations doivent être détruits, il faudra que ce soit d'une manière contrôlée.

4.6 Sécurité d'accès logique

4.6.1 L'objectif de cette politique est la maîtrise de l'accès aux informations et aux processus d'entreprise conformément aux besoins fonctionnels et aux exigences en matière de sécurité.

4.6.2 Il est tenu compte du fait que, dans le contexte de la sécurité sociale, des données confidentielles sont manipulées et qu'il est primordial de limiter l'accès aux informations et aux processus d'entreprise.

4.6.3 Des exigences fonctionnelles en matière de protection de l'accès (identification, authentification et autorisation) sont définies et documentées.

4.6.4 Des procédures sont établies pour gérer toutes les phases du cycle de vie d'une autorisation (p.ex. création, modification, contrôle, suppression).

4.6.5 L'attribution et l'utilisation de compétences critiques spéciales (ex. accès à un système d'exploitation ou à un système de base de données) sont limitées et contrôlées.

4.6.6 Les mots de passe sont gérés sur la base d'un processus formel.

4.6.7 Les mots de passe ne sont jamais stockés dans un système sous forme non sécurisée.

4.6.8 L'attention des utilisateurs est attirée sur leur responsabilité en ce qui concerne le maintien d'une protection efficace de l'accès, notamment sur le plan de l'utilisation de mots de passe et de la sécurité du matériel des utilisateurs.

4.6.9 L'accès à des services réseau internes et externes est dûment protégé.

Une attention particulière doit être accordée à la protection des accès pour le diagnostic technique à distance.

4.6.10 L'accès à des systèmes et leur utilisation sont contrôlés pour détecter les infractions à la politique d'accès ou des anomalies.

4.6.11 Pour l'accès à distance, une stratégie de protection doit être définie conformément aux risques liés à cette méthode de travail.

4.6.12 Pour l'utilisation de dispositifs de stockage mobiles[8] susceptibles de quitter le périmètre sécurisé de l'institution, une stratégie de protection adéquate doit être définie.

---

[7] Un exemple de cette altération non autorisée est le "web defacement", par lequel le contenu d'un site web est modifié dans le but de nuire au propriétaire du site web.

[8] Médias mobiles : mémoire flash amovible, disque dur portable, ordinateur portable, assistant numérique personnel (ANP).

4.7 Développement et maintenance de systèmes

4.7.1 L'objectif de cette politique est d'assurer la protection adéquate des systèmes utilisés et ce tout au cours de leur vie.

4.7.2 Pour les nouveaux systèmes ou les extensions de systèmes existants, les exigences de sécurité doivent être précisées.

4.7.3 Le développement est basé sur une approche structurée qui impose les exigences de sécurité.

4.7.4 Une attention particulière est accordée à l'élaboration de la documentation lors du développement de nouveaux systèmes et lors de la maintenance de systèmes existants.

4.7.5 Lors du développement de systèmes applicatifs, une attention particulière doit être accordée à la validation des données entrantes, à la sécurisation du traitement interne et à la validation des données sortantes.

4.7.6 Des mesures maximales sont prises pour éviter que des canaux de communication secrets se cachent dans des systèmes.

La vérification de logiciels par d'autres personnes que les développeurs constitue une méthode pour réduire ces risques.

4.7.7 Lors du développement de systèmes applicatifs, on doit tenir compte des points faibles connus sur le plan de la sécurité, propres aux langages de programmation.

La vérification de logiciels par d'autres personnes que les développeurs constitue une méthode pour réduire ces risques.

4.7.8 La protection de la confidentialité, de l'authenticité et de l'intégrité de l'information repose sur des mesures de sécurité cryptographiques adaptées (cryptage, signature numérique,...). Dans ce cadre, une attention particulière est accordée à la protection des clés cryptographiques.

Si nécessaire, ces techniques soutiennent également la non-répudiation des données.

4.7.9 L'intégrité des systèmes informatiques est garantie par une bonne gestion des logiciels sur ces systèmes opérationnels et la protection de l'accès aux bibliothèques logicielles.

4.7.10 Des procédures formelles de gestion des modifications sont utilisées pour réduire au maximum le risque d'altération de systèmes d'information. En particulier, les nouvelles versions de systèmes d'exploitation sont abordées avec la prudence nécessaire.

4.7.11 Des mesures de sécurité sont prises lorsque le développement de logiciels est confié à des tiers. Les aspects de sécurité de la collaboration sont fixés par contrat. Les modifications apportées sur les progiciels fournis par des tiers doivent être limitées au maximum.

4.7.12 Il faut garantir la confidentialité des données de test au même niveau que les données de production.

4.8 Gestion d'incidents relatifs à la sécurité de l'information

4.8.1 L'incident response team (IRT) a pour mission de réagir de façon appropriée aux incidents de sécurité. Cette équipe est chargée de réduire au maximum les dommages résultant d'incidents de sécurité et de perturbations, d'effectuer le monitoring de tels incidents et de proposer des améliorations sur la base de l'expérience acquise.

4.9 Gestion de la continuité

4.9.1 La politique de gestion de la continuité a pour but de pouvoir réagir à la perturbation des activités d'entreprise et de protéger les processus critiques d'entreprise en cas d'incidents importants. Une perturbation importante des activités opérationnelles de l'institution aurait un impact négatif sur le fonctionnement de la sécurité sociale en Belgique.

4.9.2 La gestion de la continuité est un processus documenté qui, basé sur l'analyse des risques, est constituée d'une combinaison de mesures préventives et correctives.

4.9.3 Des plans de reprise sont développés pour garantir que des processus d'entreprise puissent être rétablis dans les délais impartis.

4.9.4 Ces plans sont testés périodiquement, ce qui doit, le cas échéant, donner lieu à une correction de ceux-ci. Si nécessaire, ces plans sont testés en étroite collaboration avec l'extranet de la sécurité sociale.

4.10 Respect

4.10.1 L'institution respectera les exigences légales et contractuelles en matière de sécurité auxquelles sont soumis les systèmes d'information utilisés.

4.10.2 La situation du niveau de sécurité des systèmes d'information (y compris la révision et le suivi des procédures) sera régulièrement évaluée sur la base de la politique concernée. Cela se fera par un encadrement interne, un contrôle interne, un audit interne et/ou un audit externe.

4.10.3 Le contrôle de l'application du ISMS sera rendu possible par des outils d'aide ICT mis à la disposition d'auditeurs internes et externes.