



Security Policy

Politique de sécurité de l'information de AIM

Version 2.0

1 Définition de la sécurité de l'information

L'information est une source qui représente une valeur considérable et qui doit donc être protégée de manière appropriée. La sécurité de l'information protège l'information d'une multitude de menaces pour assurer la continuité de l'institution, limiter les dommages et contribuer au maximum à obtenir les résultats et opportunités.

La sécurité de l'information se caractérise par la garantie de la confidentialité, de l'intégrité et de la disponibilité de l'information.

En outre, la sécurité de l'information proposera des moyens pour refuser les informations falsifiées et prévenir le refus d'informations légitimes.

Dans l'AR de 1993 concernant la sécurité de l'information dans les Institutions de sécurité sociale, la sécurité de l'information est définie comme la prévention et la réparation rapide et efficace de dommages aux données sociales et de violations illégitimes de la vie privée des intéressés.

2 Objectif de la sécurité de l'information de AIM

AIM (Agence Intermutualiste) est une asbl qui a été fondée en octobre 2002, par les sept organismes assureurs. Ses statuts (annexe 3) ont été revus en décembre 2003.

L'objectif de AIM, en conformité avec la loi-programme I du 24 décembre 2002 (annexe 1), consiste-en

« Analyser dans le cadre des missions des organismes assureurs les données qu'ils collectent et fournir les informations à ce propos ».

Le « mission statement » et les critères de sélection des missions de AIM font l'objet d'un document (annexe 4).

La sécurité de l'information de AIM vise à garantir le bon fonctionnement des activités de AIM en cohérence avec ses missions.

De manière plus générale, elle a en outre comme objectif de prévenir les dommages qui peuvent toucher le bon fonctionnement et la confidentialité des systèmes d'information de la sécurité sociale d'une part ainsi que la protection et la confidentialité de la vie privée des intéressés d'autre part.

En effet, l'informatisation des institutions de sécurité sociale et la collaboration croissante offrent d'énormes progrès sur le plan de l'effectivité et de l'efficacité mais donnent en même temps naissance à de nouveaux risques. Les institutions distinctes de sécurité sociale ne sont plus des entités indépendantes de traitement de l'information, mais font partie d'un groupe cohérent. Les liens de collaboration



Security Policy

en évolution augmentent considérablement le risque et l'ampleur de dommages réfléchis sur d'autres systèmes que celui victime du dommage de base. C'est pourquoi la vision en matière de sécurité de l'information, de confidentialité de l'information, de protection de la vie privée et de confidentialité de la vie privée est définie communément.

Une perturbation importante de la sécurité de l'information de AIM pourrait avoir un impact négatif sur le fonctionnement de la sécurité sociale.

La sécurité de l'information s'obtient par la mise en œuvre d'une série de mesures politiques ou de contrôles (fonctions hardware et software, processus, procédures, structures organisationnelles). Ceux-ci doivent être mis au point pour réaliser les objectifs de sécurité de l'organisation.

La politique de sécurité doit reposer sur un modèle en couches impliquant plusieurs mesures complémentaires. La sécurité qui peut être atteinte par des moyens techniques ne constitue qu'une des couches. Ces moyens doivent aussi être complétés par un système de gestion efficace et par les processus nécessaires. Un élément fondamental pour une bonne sécurité de l'information est la participation de tous les collaborateurs dans l'entreprise. De même, le concours des fournisseurs, des clients et des partenaires d'entreprise est important.

Le système intégré qui permet d'aboutir à une sécurité maximale de l'information est un ISMS (Information Security Management System).

2.1 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 satisfaites. Ces dispositions concernées sont mentionnées en annexe 1.



Security Policy

3 Approche générale de la sécurité de l'information de AIM

3.1 Approche générale de la sécurité de l'information

Le système intégré qui doit permettre d'aboutir à une sécurité maximale de l'information (ISMS) est basé sur la norme ISO 17799.

Dans ce cadre, il est tenté de trouver un équilibre objectif entre les mesures préventives (prévention d'incidents de sécurité), répressives (limitation des conséquences négatives d'incidents) et correctives.

Voici une approche générale qui peut être résumée comme ceci :

Politique de sécurité de l'information – Définition de la portée

Revoir régulièrement la "Politique de sécurité de l'information" et la diffuser dans l'organisation. La portée (scope) de la politique doit être définie en termes d'organisation, de localisation et de ressources.

Organisation de la sécurité

Adapter l'organisation de la sécurité aux besoins en évolution avec une désignation claire de responsabilités, tâches et compétences.

Exigence de sécurité – inventaire des ressources – analyse des risques

Définir les exigences en matière de sécurité pour les ressources dans la portée de la politique de sécurité, réaliser un inventaire et une analyse des risques.

Sélection et mise en œuvre des contrôles

Sélectionner et mettre en œuvre les contrôles de sécurité pour prévenir les risques. Les coûts des mesures de sécurité doivent être en équilibre tant avec la valeur de la ressource pour l'entreprise qu'avec le dommage que puisse causer un incident.

Planning de continuité

Le planning de continuité est axé sur la poursuite des processus critiques d'entreprise.

Training et formation

Un programme de formation est prévu pour former les collaborateurs à manier les informations et les systèmes ICT (Information and communication technology) avec soin et vigilance.

Documentation et déclaration d'applicabilité

Contrôle, audit, évaluation et amélioration

La surveillance des mesures de sécurité peut être complétée par un audit interne et externe et des actions d'amélioration peuvent en découler.

3.2 Plan de révision périodique



Security Policy

Le document « Politique de sécurité de l'information de AIM » fera l'objet d'une révision annuelle.



Security Policy

4 Politique de la sécurité de l'information de AIM

Introduction

Dans un ISMS, la « Politique de sécurité de l'information » est un document de base important car c'est dans ce document que sont énoncés les principes fondamentaux de la sécurité de l'information que doit respecter chaque collaborateur.

Les paragraphes suivants représentent de manière générale, les principales mesures politiques qui cadrent dans le ISMS de AIM. Il est donc important que chaque collaborateur de l'entreprise connaisse le contenu de ce document.

Les divers aspects mentionnés dans cette charte seront détaillés, si nécessaire, dans des documents politiques spécifiques (« polices »).

Ce document sera revu périodiquement, après l'évaluation de la politique à l'occasion d'incidents de sécurité importants, de nouvelles vulnérabilités ou de changement dans l'infrastructure organisationnelle ou technique.

Portée

- La « politique de sécurité de l'information » s'applique à tous les systèmes d'information développés, opérationnels et à développer dans tous les « sites » de AIM ou dans tous les « sites » appelés à traiter de l'information de AIM.
- La « politique de sécurité de l'information » s'applique à tous les collaborateurs appelés à traiter de l'information dans le cadre d'un projet de AIM.
- La « politique de sécurité de l'information » s'applique aux collaborateurs externes (sous-traitants, consultants, fournisseurs,...) occupés temporairement ou sous durée indéterminée par AIM.

4.1 Organisation de la sécurité

1. La politique liée à l'organisation de la sécurité a pour objectif de gérer la sécurité de l'information au sein de l'organisation.
2. AIM devra veiller à élaborer et à maintenir la politique de sécurité : révision de cette politique, ajout de mesures de sécurité, établissement de plans de sécurité, détermination des responsabilités et surveillances des incidents de sécurité en évolution.
3. AIM devra réagir de façon appropriée aux incidents de sécurité et devra les consigner.



Security Policy

4. AIM devra veiller à minimaliser le dommage résultant d'incidents de sécurité et de perturbations, contrôler de tels incidents et introduire des améliorations sur base de l'expérience acquise.
5. Dans ce cadre sont désignées et attribuées les responsabilités pour la sécurité de l'information.
6. Une attention particulière est accordée aux aspects organisationnels de la collaboration avec des tiers. Les aspects de sécurité de la collaboration sont définis dans des contrats.

4.2 Classification et gestion des ressources

Dans ce contexte, les ressources consistent notamment en hardware, en software et en données.

1. La politique relative à la classification et à la gestion des ressources a pour objet le maintien d'une protection adéquate de ces ressources.
2. Il est tenu compte du fait que des données confidentielles sont manipulées. Le traitement de ces données est soumis à la législation et autres dispositions connexes (contractuelles, réglementaires, ...).

4.3 Sécurité liée aux collaborateurs

Cette politique a pour but d'utiliser le mieux possible et de maintenir au niveau requis la connaissance et l'expérience des collaborateurs pour promouvoir la sécurité, ainsi que réduire les risques d'erreurs humaines délibérées ou non.

Voir Annexe 2.

4.4 Sécurité physique et de l'environnement

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, la modification, la manipulation ou le vol d'informations. Elle a aussi pour but de prévenir le dommage ou la perturbation de systèmes d'information.

Les règles suivantes sont recommandées pour un contrôle minimum des accès physiques :

- l'accès physique toujours fermé,
- un système de contrôle d'accès par code électronique, badge ou identification,
- un système de détection d'intrusion en dehors des heures et jours ouvrables.

4.5 Gestion opérationnelle

Cette politique vise à garantir un service et un fonctionnement corrects et sûrs des infrastructures et processus ICT.

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



Security Policy

Grâce à une planification des capacités et des procédures d'acceptation adéquates pour les systèmes ICT neufs et modifiés, le risque de perturbation des systèmes est limité au maximum.

Afin d'assurer la protection de l'intégrité des logiciels et des informations, des mesures sont prises pour prévenir, découvrir des logiciels nuisibles et en limiter aux mieux les conséquences éventuelles.

De même, les signalements de nouvelles menaces sont suivis par des instances compétentes et les mesures nécessaires sont prises (patches software) sans compromettre la continuité.

Des responsabilités et des procédures sont définies :

- pour le contrôle de toutes les modifications aux appareils, logiciels et procédure,
- pour le traitement des incidents : communiquer, consigner et réagir.

Les environnements pour le développement, les tests et la production sont séparés.

Dans les cas où il existe un risque à la sécurité, les fonctions sont séparées pour réduire le risque suite à un manquement ou un abus délibéré de systèmes.

Avant que les moyens ICT entrent en phase opérationnelle, il est vérifié que toutes les exigences vis-à-vis de ces moyens (fonctionnalité, sécurité, ...) sont implémentées et testées.

Selon les consignes de sécurité concernées, des backups d'informations essentielles et de logiciels doivent régulièrement être effectués pour garantir l'intégrité et la disponibilité des services.

Une attention particulière est accordée au maintien de la sécurité de l'information en réseau et la protection de l'infrastructure sous-jacente. Des mesures maximales et adaptées sont prises lors du transport de données sensibles via des réseaux publics.

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

Dans le respect des règles légales en matière de conservation et d'utilisation des données archivées, chaque évolution de l'infrastructure informatique et du système d'information nécessitent une complète vérification de l'adéquation entre les données archivées, les supports de stockage utilisés et les applications nécessaires à leurs utilisations.

Des mesures sont prises pour éviter la perte, la modification ou le vol d'informations échangées avec d'autres organisations.

Une certaine attention est accordée à la protection de l'intégrité de l'information sur des systèmes accessibles au grand public (tels que les serveurs web) pour éviter



Security Policy

l'accès et des modifications non autorisées susceptibles de nuire à la réputation de AIM.

Une attention particulière est également accordée aux risques de l'utilisation de l'internet et de courriels.

En cas d'assignation d'activités ICT à une entreprise externe, une attention supplémentaire est accordée aux risques envers la sécurité. Les aspects de sécurité sont traités par contrat.

4.6 Sécurité d'accès logique

L'objectif de cette politique est la maîtrise de l'accès aux informations et processus d'entreprise sur base des besoins et exigences en matière de sécurité.

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

Les contraintes liées à la sécurité d'accès sont définies et documentées.

Les contrôles d'accès logiques suivants interviennent pour un contrôle minimum des accès logiques :

Identification et authentification des utilisateurs :

Des procédures formelles sont établies pour maîtriser toutes les phases dans le cycle de vie d'une autorisation (introduction, contrôle, annulation).

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

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

L'attribution et l'utilisation de compétences spéciales critiques(ex : accès à une base de données relatives à la santé) sont limitées et contrôlées.

Les utilisateurs se voient souligner leur responsabilité pour le maintien d'une sécurité d'accès efficace, notamment concernant l'utilisation de mots de passe et la sécurité du matériel utilisé.

Définition et protection des ressources :

Les ressources sont des données, des programmes ou du texte, elles sont confidentielles et de ce fait, leur manipulation et leur accès font partie d'un processus formel.

Administration des accès aux données :

Seul un utilisateur ayant toutes les autorisations nécessaires peut donner, modifier, supprimer des autorisations d'accès.



Security Policy

Un enregistrement des tentatives d'accès sera mis en place.

L'accès par réseaux à des services réseaux internes et externes est protégé efficacement.

Des mesures spécifiques sont élaborées pour la sécurité d'accès pour les systèmes d'exploitation et pour des applications.

Pour l'utilisation d'ordinateurs portables et l'organisation du télétravail, une stratégie de sécurité doit être établie en accord avec les risques liés à ce mode de travail.

4.7 Développement et maintenance de systèmes

L'objectif de cette politique est de garantir que les systèmes utilisés offrent la sécurité requise tout au long du cycle de vie.

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.

Le développement est basé sur un processus qui impose des exigences en matière de sécurité. Il est tenu compte des points faibles connus sur le plan de la sécurité, propre aux langages de programmation. De plus, une attention particulière est consacrée à la validation des données input, la sécurisation du traitement interne et à la validation des données output. Voir 4.5.

Des procédures formelles pour la gestion des modifications sont utilisées pour réduire au maximum le risque d'altération du système d'information.

Des mesures de sécurité pour tout développement « outsourcé » doivent être mises en place. Les logiciels fournis par des tiers doivent être utilisés le plus possible de manière inchangée.

La confidentialité des données de test doit être garantie au même niveau que les données de production.

L'intégrité des systèmes informatiques est garantie par une bonne gestion des logiciels sur systèmes opérationnels et la sécurité d'accès pour les bibliothèques software.

4.8 Règles de publication des informations

Annexe 5

4.9 Gestion de la continuité

La politique de la gestion de la continuité a pour but de pouvoir réagir à la perturbation d'activités d'entreprise et de protéger les processus critiques



Security Policy

d'entreprise en cas d'incidents importants et ce en fonction de l'importance des applications en question et dans des délais appropriés aux exigences spécifiques.

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

Des plans de continuité sont développés pour garantir que des processus d'entreprises peuvent être rétablis dans des délais impartis. Ils seront testés périodiquement.

4.10 Respect des exigences légales et contractuelles

AIM respectera les exigences légales et contractuelles en matière de sécurité auxquelles sont soumis les systèmes d'information utilisés (voir annexe6 : législation sur la sécurité d'information, sécurité des télécommunications, vie privé, fraude informatique, ...).



Security Policy

5 Références

ISO/IEC 17799: 2000 Information technology – Code of practice for information security management.

Beleid voor Informatieveiligheid (Information Security Policy) version 0.3 van KCE (Fédéraal Kenniscentrum voor gezondheidzorg).

BCSS (Banque Carrefour de la sécurité Sociale) - Sécurité – Information Security Management System



Security Policy

6 Tableau récapitulatif des documents et actions.

Document Tableau récapitulatif des documents et actions dans le cadre de la Politique de sécurité de l'information AIM.

	Politique_securite_information_AIM.doc
	Lois sécu IMA_FR.doc
	Security IMA Instructions pour collaborateurs.doc
	Demande d'accès par le PM FR.doc



Security Policy

Annexe 1 : Législation sur la sécurité de l'information

Cette législation évolue régulièrement. Pour le dernier statut, prière de consulter les http mentionnés.

Intitulés et textes :

Législation spécifique à la sécurité sociale :

- [Loi du 15.01.1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale ;](#)
- [Arrêté royal du 04.02.1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale ;](#)
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1997020448%2FF&caller=list&row_id=1&numero=8&rech=9&cn=1997020448&la=F&sql=dt+contains+++%27ARRETE%27%26+%27ROYAL%27+and+dd+between+date%271997-02-04%27+and+date%271997-02-04%27+&language=fr&trier=promulgation&dt=ARRETE+ROYAL+&fromtab=loi&ddda=1997&tri=dd+AS+RANK+&imgcn.x=33&imgcn.y=9
- [Arrêté royal du 12.08.1993 relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale ;](#)
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1993081230%2FF&caller=list&row_id=1&numero=1&rech=13&cn=1993081230&la=F&sql=dt+contains+++%27ARRETE%27%26+%27ROYAL%27+and+dd+between+date%271993-08-12%27+and+date%271993-08-12%27+&language=fr&trier=promulgation&dt=ARRETE+ROYAL+&fromtab=loi&ddda=1993&tri=dd+AS+RANK+&imgcn.x=49&imgcn.y=9
- [Loi-programme I du 24.12.2002 : articles 259 à 300 relatifs au KCE et IMA.](#)
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=2002122431%2FF&caller=list&row_id=1&numero=8&rech=8&cn=2002122431&la=F&sql=dt+contains+++%27LOI%27+and+dd+between+date%272002-12-24%27+and+date%272002-12-24%27+&language=fr&dddj=24&trier=promulgation&dt=LOI+&dddm=12&fromtab=loi&ddda=2002&ddfa=2002&tri=dd+AS+RANK+&imgcn.x=61&imgcn.y=12

NB : pour votre info, les textes de ces dispositions sont repris dans le document « Législations en rapport avec la sécurité de l'information ». (Lois secu IMA_FR_net1.doc) (veilig wetten IMA)



Security Policy

Protection de la vie privée :

- **[Loi du 08.12.1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel](#)** ;
- **[Arrêté royal du 13.02.01 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel](#)** ;
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=2001021332%2F&caller=list&row_id=1&numero=3&rech=3&cn=2001021332&la=F&sql=dt+contains+++%27ARRETE%27%26+%27ROYAL%27+and+dd+between+date%272001-02-13%27+and+date%272001-02-13%27+&language=fr&trier=promulgation&dt=ARRETE+ROYAL+-&fromtab=loi&ddda=2001&tri=dd+AS+RANK+&imgcn.x=54&imgcn.y=11
- **[Loi du 08.08.1983 organisant un registre national des personnes physiques](#)** ;
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1983080836%2F&caller=list&row_id=1&numero=2&rech=2&cn=1983080836&la=F&sql=dt+contains+++%27LOI%27+and+dd+between+date%271983-08-08%27+and+date%271983-08-08%27+&language=fr&dddj=08&trier=promulgation&dt=LOI+-&dddm=08&fromtab=loi&ddda=1983&ddfa=1983&tri=dd+AS+RANK+&imgcn.x=41&imgcn.y=9
- **[Loi du 30.06.1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées](#)** ;
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1994063049%2F&caller=list&row_id=1&numero=9&rech=9&cn=1994063049&la=F&chercher=t&language=fr&trier=promulgation&choix1=ET&choix2=ET&ddda=1994&ddfa=1994&tri=dd+AS+RANK+&dddj=30&fr=f&dt=LOI+-&dddj=30&dddm=06&ddfm=06&set1=SET+TERM_GENERATOR+%27word%21ftelp%2Flang%3Dfrench%2Fbase%2Froot%2Fderive%2Finfect%27&set3=set+character_variant+%27french.ftl%27&fromtab=loi&sql=dt+contains+++%27LOI%27+and+dd+between+date%271994-06-30%27+and+date%271994-06-30%27+&imgcn.x=46&imgcn.y=10

NB : pour votre info, les textes de ces dispositions sont repris dans le document « Législations en rapport avec la sécurité de l'information ». (Lois secu IMA_FR_net1.doc) (veilg wetten IMA)



Security Policy

Autres intitulés :

Fraude informatique :

- **[Loi du 28 novembre 2000 relative à la criminalité informatique.](http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=2000112834%2FF&caller=list&row_id=1&numero=1&rech=2&cn=2000112834&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%272000-11-28%27+and+date%272000-11-28%27+&language=fr&dddj=28&trier=promulgation&dt=LOI+&dddm=11&fromtab=loi&ddd=2000&ddfa=2000&tri=dd+AS+RANK+&imgcn.x=60&imgcn.y=6)**
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=2000112834%2FF&caller=list&row_id=1&numero=1&rech=2&cn=2000112834&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%272000-11-28%27+and+date%272000-11-28%27+&language=fr&dddj=28&trier=promulgation&dt=LOI+&dddm=11&fromtab=loi&ddd=2000&ddfa=2000&tri=dd+AS+RANK+&imgcn.x=60&imgcn.y=6

Protection des programmes d'ordinateurs :

- **[Loi du 30.06.1994 relative au droit d'auteur et aux droits voisins ;](http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1994063035%2FF&caller=list&row_id=1&numero=8&rech=9&cn=1994063035&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%271994-06-30%27+and+date%271994-06-30%27+&language=fr&dddj=30&trier=promulgation&dt=LOI+&dddm=06&fromtab=loi&ddd=1994&ddfa=1994&tri=dd+AS+RANK+&imgcn.x=44&imgcn.y=11)**
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1994063035%2FF&caller=list&row_id=1&numero=8&rech=9&cn=1994063035&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%271994-06-30%27+and+date%271994-06-30%27+&language=fr&dddj=30&trier=promulgation&dt=LOI+&dddm=06&fromtab=loi&ddd=1994&ddfa=1994&tri=dd+AS+RANK+&imgcn.x=44&imgcn.y=11
- **[Loi du 30.06.1994 transposant en droit belge la directive européenne du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur.](http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1994063036%2FF&caller=list&row_id=1&numero=4&rech=9&cn=1994063036&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%271994-06-30%27+and+date%271994-06-30%27+&language=fr&dddj=30&trier=promulgation&dt=LOI+&dddm=06&fromtab=loi&ddd=1994&ddfa=1994&tri=dd+AS+RANK+&imgcn.x=45&imgcn.y=5)**
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1994063036%2FF&caller=list&row_id=1&numero=4&rech=9&cn=1994063036&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%271994-06-30%27+and+date%271994-06-30%27+&language=fr&dddj=30&trier=promulgation&dt=LOI+&dddm=06&fromtab=loi&ddd=1994&ddfa=1994&tri=dd+AS+RANK+&imgcn.x=45&imgcn.y=5

Banque de données :

- **[Loi du 31.08.1998 transposant en droit belge la directive européenne du 11 mars 1996 concernant la protection juridique des bases de données.](http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1998083141%2FF&caller=list&row_id=1&numero=1&rech=2&cn=1998083141&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%271998-08-31%27+and+date%271998-08-31%27+&language=fr&dddj=31&trier=promulgation&dt=LOI+&dddm=08&fromtab=loi&ddd=1998&ddfa=1998&tri=dd+AS+RANK+&imgcn.x=37&imgcn.y=11)**
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=1998083141%2FF&caller=list&row_id=1&numero=1&rech=2&cn=1998083141&la=F&sql=dt+contains+%27LOI%27+and+dd+between+date%271998-08-31%27+and+date%271998-08-31%27+&language=fr&dddj=31&trier=promulgation&dt=LOI+&dddm=08&fromtab=loi&ddd=1998&ddfa=1998&tri=dd+AS+RANK+&imgcn.x=37&imgcn.y=11



Security Policy

Droit social :

- [Convention collective de travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.](#)

Autres législations connexes :

- [Loi du 09.07.2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification ;](http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=2001070943%2FF&caller=list&row_id=1&numero=1&rech=2&cn=2001070943&la=F&sql=dt+contains++%27LOI%27+and+dd+between+date%272001-07-09%27+and+date%272001-07-09%27+&language=fr&dddj=09&trier=promulgation&dt=LOI+&dddm=07&fromtab=loi&ddda=2001&ddfa=2001&tri=dd+AS+RANK+&imgcn.x=56&imgcn.y=10)
http://www.juridat.be/cgi_loi/loi_a1.pl?DETAIL=2001070943%2FF&caller=list&row_id=1&numero=1&rech=2&cn=2001070943&la=F&sql=dt+contains++%27LOI%27+and+dd+between+date%272001-07-09%27+and+date%272001-07-09%27+&language=fr&dddj=09&trier=promulgation&dt=LOI+&dddm=07&fromtab=loi&ddda=2001&ddfa=2001&tri=dd+AS+RANK+&imgcn.x=56&imgcn.y=10
- [Loi du 10.01.1990 concernant la protection juridique des topographies de produits semi-conducteurs.](#)



Security Policy

Annexe 2 : Sécurité liée aux collaborateurs

Voir Policy « Gegevensbeiliging en beroepsgeheim » - richtlijnen medewerkers.



Security Policy

Annexe 3 : Statuts

<http://www.nic-ima.be/library/documents/presentation/Nieuwe%20Statuten%20IMA%20%20RvB%20IMA%20van%2016.12.2003.pdf>



Security Policy

Annexe 4 : Agence Intermutualiste Mission Statement et Critères de Sélection des missions

[http://www.nic-
ima.be/library/documents/presentation/Mission%20statement%20F%20IMA%202005%2001%2020\(1\).pdf](http://www.nic-ima.be/library/documents/presentation/Mission%20statement%20F%20IMA%202005%2001%2020(1).pdf)



Security Policy

Annexe 5 : Règles de publication des informations

Voir Document spécifiant les règles de publication des informations.