Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Guide pour l'élaboration d'une politique de sécurité de système d'information

PSSI

SECTION 4
RÉFÉRENCES SSI

Version du 3 mars 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Objet de la modification	Statut
15/09/1994 (1.1)	Publication du guide d'élaboration de politique de sécurité interne (PSI).	Validé
2002	Révision globale : - actualisation des références, - création d'une méthodologie, - enrichissement et reclassement des principes de sécurité, - séparation en 3 sections (méthodologie, principes de sécurité et compléments).	Draft
2003	Restructuration, remise en forme, amélioration de la méthode, mise en cohérence avec les outils méthodologiques et meilleures pratiques de la DCSSI suite à une consultation d'experts internes.	Prétest
23/12/2003	Séparation en 4 sections (introduction, méthodologie, principes de sécurité et références SSI) et améliorations diverses suite à une consultation d'experts externes (notamment le Club EBIOS) et à plusieurs mises en pratique (ministère de la Défense, CNRS, Direction des Journaux Officiels…).	Prétest pour validation
03/03/2004	Publication du guide pour l'élaboration d'une politique de sécurité de système d'information (PSSI)	Validé

Table des matières

Introduction

Le guide PSSI est décomposé en quatre sections :

- l'introduction permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ;

- la méthodologie présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ;

- le référentiel de principes de sécurité ;

- une liste de documents de références de la SSI (ce document, présentant les critères d'évaluation, les textes législatifs, les normes, les codes d'éthiques, les notes complémentaires...).

L'attention du lecteur est attirée sur le fait que les sections composant le guide PSSI seront mises à jour indépendamment.

Un formulaire de recueil de commentaires figure en annexe de chaque guide afin de renvoyer des propositions et remarques à la DCSSI.

Objet du document

Avertissement :

Le contenu de la présente section est donné à titre indicatif et n'est pas exhaustif. Par conséquent, le lecteur est invité - tout particulièrement pour les textes juridiques cités – à vérifier leur validité ainsi que la parution éventuelle de nouveaux textes.

Cette section du guide PSSI présente les références SSI suivantes :

- **critères d'évaluation** : présentation de l'ISO/IEC 15408 (critères communs), norme internationale permettant d'évaluer concrètement la SSI avec une approche commune et reconnue ;

- **lignes directrices de l'OCDE** : principes de base en matière de SSI et de cryptographie édictés par l'Organisation du Commerce et du Développement Économique ;

- **codes d'éthique des métiers des technologies de l'information** : exemples pour l'aide à l'élaboration d'un code d'éthique ;

- **textes législatifs et réglementaires/recommandations** : textes de lois et recommandations, présentés dans une perspective de droit pénal :
  - les atteintes aux personnes,
  - les atteintes aux biens,
  - les atteintes aux intérêts fondamentaux de la nation, terrorisme et atteintes à la confiance publique,
  - les atteintes à la propriété intellectuelle,
  - les dispositions relatives à la cryptologie,
  - les dispositions relatives à la signature électronique ;

- **autres textes** : réglementation et guides divers.

1 Les Critères Communs pour l'évaluation de la sécurité des technologies de l'information

L'évaluation selon les critères communs peut concerner un système dont l'environnement d'exploitation est connu dès la conception ou un produit proposé sur catalogue et pour lequel ne peuvent être faites que des hypothèses sur son environnement d'utilisation.

L'évaluation d'un système ou d'un produit permet d'obtenir l'assurance qu'il fournit une sécurité adéquate pour satisfaire ses objectifs de sécurité. Il est prévisible qu'à moyen terme de nombreux produits certifiés seront disponibles pour répondre aux besoins des utilisateurs. Ceux-ci pourront, par exemple, utiliser des produits certifiés qui leur conviennent pour la conception d'un système ; ils pourront aussi inclure des produits certifiés dans un système existant. Ces évaluations selon les critères communs nécessitent un examen approfondi du système ou du produit, depuis sa conception jusqu'à son exploitation courante. L'expression anglaise "*target of evaluation*" est traduite par cible d'évaluation ; elle est utilisée dans les critères communs pour désigner le système ou le produit à évaluer et qui est une implémentation de la cible de sécurité.

Afin de répondre à ce besoin croissant de confiance des utilisateurs dans la sécurité offerte par les technologies de l'information, le gouvernement a institué par le décret no 2002-535 du 18 avril 2002 un schéma national d'évaluation et de certification permettant aux acteurs étatiques et privés de faire réaliser des évaluations sécuritaires par une tierce partie indépendante, sous contrôle d'un organisme de certification gouvernemental (la DCSSI). Ces tierces parties indépendantes sont des centres d'évaluations agréés par la DCSSI.

1.1 Les acteurs

La démarche des critères communs identifie trois acteurs principaux qui sont concernés par l'évaluation et définit leurs responsabilités respectives :

- le **commanditaire** de l'évaluation est l'autorité propriétaire du système ou du produit qui définit les besoins à satisfaire et qui est à l'origine de la demande d'évaluation. Il doit définir la cible de sécurité pour l'évaluation ; le commanditaire et le développeur peuvent être confondus,

- le **développeur** est la personne qui réalise la cible d'évaluation compte tenu de l'expression de besoins du commanditaire,

- l'**évaluateur** est la personne qui effectue l'évaluation de la sécurité.

Dans le cadre du schéma, l'organisme de certification pilote le processus d'évaluation et de certification.

Une évaluation nécessite la collaboration de ces trois acteurs, si possible dès le début du développement de la cible d'évaluation. Autant pour préserver le maximum d'objectivité dans les résultats d'une évaluation que pour réduire la charge et les frais de l'évaluation, il est prévu que le commanditaire fournisse les éléments de preuve exigés. Ceux-ci sont vérifiés par l'évaluateur qui doit aussi effectuer des tests complémentaires. L'organisme certificateur valide l'ensemble des travaux réalisés par l'évaluateur, demande éventuellement des informations et travaux complémentaire afin d'avoir l'ensemble des éléments de preuves nécessaires pour procéder ensuite à la certification du produit ou du système.

1.2 La cible de sécurité

Cette cible qui a été définie par le commanditaire et qui peut être utilisée pour le développement du système ou du produit, contient tous les renseignements relatifs aux spécifications de la sécurité.

C'est l'étape fondamentale de la conception d'un système selon les principes exposés dans la première partie ; c'est la référence de base pour l'évaluation selon les critères communs.

Cette cible caractérise la politique de sécurité du système et elle contient :

- les objectifs de sécurité,
- les exigences de sécurité qui en découlent :
  - les exigences fonctionnelles de sécurité : fonctionnalités devant être implémentées dans le produit pour réaliser les objectifs,
  - les exigences d'assurance de sécurité (le niveau d'évaluation) : mesures permettant de s'assurer que le produit répond aux objectifs,
- les fonctions de sécurité offertes par le produit ou le système.

1.3 Les exigences fonctionnelles

Pour réaliser les objectifs de sécurité identifiés, la cible de sécurité doit comporter des exigences fonctionnelles qui précisent les fonctionnalités de sécurité qui doivent être implémentées dans le produit ou le système évalué.

Ces exigences sont regroupées dans la deuxième partie des critères communs suivant onze rubriques génériques:
- audit de sécurité (FAU),
- communication (FCO),
- support cryptographique (FCS),
- protection des données de l'utilisateur (FDP),
- identification et authentification (FIA),
- gestion de la sécurité (FMT),
- protection de la vie privée (FPR),
- protection des fonctions de sécurité de la cible d'évaluation (FPT),
- utilisation des ressources (FRU),
- accès à la cible d'évaluation (FTA),
- chemins et canaux de confiance (FTP).

1.4 Les exigences d'assurance

Les exigences d'assurance définissent les critères à appliquer pour l'évaluation du produit ou du système. Ces exigences sont tirées de la partie 3 des critères communs :
- analyse de la gestion de configuration (ACM),
- analyse des livraison et exploitation (ADO),
- analyse du développement (ADV),
- analyse des guides d'utilisation et d'exploitation (AGD),
- analyse du support au cycle de vie (ALC),
- analyse et réalisation des tests fonctionnels (ATE),
- analyse et réalisation de l'estimation des vulnérabilités, et tests pour exploiter les vulnérabilités identifiées (AVA),
- maintenance de l'assurance (AMA).

Le niveau d'assurance (EAL), correspond à une sélection particulière d'exigences d'assurance.

Le résultat de l'évaluation est une confirmation ou une infirmation que la cible d'évaluation satisfait ses objectifs de sécurité avec la confiance correspondante au niveau d'évaluation visé. La découverte d'une vulnérabilité exploitable pour le niveau considéré met en échec l'évaluation.

La certification est délivrée par l'organisme de certification lorsque l'ensemble des travaux d'évaluation a permis d'établir que le produit ou système rencontre les objectifs de sécurité et ne comporte pas de vulnérabilités exploitables.

1.5 Conclusion

Les critères communs proposent une approche méthodique et cohérente pour examiner la façon dont est prise en compte la sécurité dans la conception, le développement et l'exploitation d'un système d'information. Cette approche exige en particulier que les objectifs de sécurité aient été définis au préalable pour que l'on puisse apprécier, grâce à l'évaluation, la manière dont les fonctions de sécurité parviennent à les satisfaire.

L'élaboration de ces critères a été guidée par le souci de préserver le maximum d'objectivité dans les résultats d'une évaluation. Ils sont utilisables pour l'évaluation d'une gamme très large de produits de sécurité et de systèmes d'information sécurisés. De plus, leur adoption par la communauté

internationale (les critères communs ont été normalisés par l'ISO en 1999 : ISO/IEC 15408) est favorable au développement du marché de la sécurité.

Ils constituent la pièce importante de l'œuvre de sécurisation dont l'objectif est d'améliorer la sécurité et, pour cela, de faire naître un marché de produits développés conformément aux besoins des utilisateurs.

Il est important que les utilisateurs soient bien persuadés que seule une approche globale comme celle qui a été présentée ci-dessus peut permettre de bien gérer le problème de la sécurité du traitement de l'information, problème qui ne peut être résolu que s'il a été clairement défini.

2 Les lignes directrices de l'OCDE

2.1 Lignes directrices régissant la sécurité des systèmes et réseaux d'information

Adoptée par le Conseil de l'OCDE lors de sa 1037ème session le 25 juillet 2002, la version du 29 juillet 2002 des "lignes directrices régissant la sécurité des systèmes et réseaux d'information – vers une culture de la sécurité" fait l'objet d'une recommandation de portée internationale.
Les lignes directrices ont pour but de :

- promouvoir la culture de sécurité,
- renforcer la sensibilisation aux risques,
- politiques, pratiques, mesures et procédures SSI,
- améliorer la confiance envers les SI,
- créer un cadre de référence cohérent pour appréhender la SSI et respecter des valeurs éthiques,
- promouvoir la coopération et le partage d'informations relatives à la SSI,
- promouvoir la prise en considération de la SSI et l'élaboration de normes.

Les lignes directrices se présentent sous la forme de neuf principes qui se complètent et doivent être considérés comme un tout. Chaque principe fait l'objet d'une description succincte figurant ci-après et d'un paragraphe de développement.

Sensibilisation
"Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité."

Responsabilité
"Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information."

Réaction
"Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité."

Éthique
"Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes."

Démocratie
"La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique."

Évaluation des risques
"Les parties prenantes doivent procéder à des évaluations des risques."

Conception et mise en œuvre de la sécurité
"Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information."

Gestion de la sécurité
"Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité."

Réévaluation
"Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité."

Depuis septembre 2002, le Secrétariat général de la défense nationale (SGDN), et plus particulièrement la Direction centrale de la sécurité des systèmes d'information (DCSSI) publie un mémento relatif à ces nouvelles lignes directrices sur son site web (http://www.ssi.gouv.fr/fr/actualites/archives.html).

De plus, la publication des lignes directrices a été annoncée lors de la commission interministérielle de la sécurité des systèmes d'information (CISSI) du 26 septembre 2002.
La France a déjà mis en œuvre un grand nombre de mesures visant à promouvoir la culture de sécurité. Elles s'inscrivent parfaitement dans les actions répertoriées dans le plan d'application des lignes directrices de l'OCDE.

Politique nationale visant la sécurité de l'information

La France a mis en place et tient à jour un cadre juridique visant à garantir la sécurité des systèmes d'information et prenant en compte l'évolution de la société de l'information.

Dès 1988, la loi « Godfrain » avait complété le dispositif pénal existant en sanctionnant les actes de vandalisme appliqués aux systèmes d'information, permettant ainsi de lutter contre des formes de criminalité informatique telles que les virus, les bombes logiques ou les «chevaux de Troie » (logiciels espions ayant pour but de surveiller un site ou un système informatique, voire de le contrôler à distance).

D'autre part, un projet de loi récent sur la société de l'information, en cours de préparation, prévoit de renforcer cet arsenal juridique et d'aggraver les peines sanctionnant le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données, d'en entraver ou d'en fausser le fonctionnement, et d'y introduire ou d'y supprimer frauduleusement des données.

Cet arsenal juridique est conforme à la Convention sur la cybercriminalité du Conseil de l'Europe, signée par la France en 2001 et en cours de ratification, et au projet européen de décision cadre relatif aux attaques visant des systèmes d'information, en cours de discussion au Conseil de l'Union européenne et au Parlement européen.

Coopération transfrontière

La France est l'un des premiers pays à avoir appartenu au réseau 24/7 mis en place par le G8 à l'origine et qui relie actuellement 29 pays. Ce réseau transfrontière que les pays membres peuvent activer à tout moment doit permettre de faciliter les contacts en cas d'urgence. L'idée de ce réseau a d'ailleurs été reprise dans la Convention sur la cybercriminalité du Conseil de l'Europe.

Diffusion des alertes et notes d'information

Le CERTA est une structure d'alerte et d'assistance sur l'Internet, chargée d'une mission de veille et de réponse aux attaques informatiques. Les deux principaux objectifs du CERTA sont d'assurer la détection des vulnérabilités et la résolution d'incidents concernant la sécurité des systèmes d'information (SSI) ainsi que l'aide à la mise en place de moyens permettant de se prémunir contre de futurs incidents.

Pour ce faire, le CERTA met à disposition du public sur son site web :

- des alertes destinées à prévenir un danger immédiat,
- des avis faisant état de vulnérabilités et de moyens de s'en prémunir,
- des notes d'information faisant état de phénomènes à porter générale,
- des recommandations.

En effet, le CERTA a été mis en place pour renforcer et coordonner la lutte contre les systèmes informatiques de l'État.

Sensibilisation et mise à disposition de méthodes de sécurisation des systèmes informatiques

Les travaux du bureau conseil de la DCSSI appliquent les principes contenus dans les nouvelles lignes directrices de l'OCDE. On peut citer entre autres :

- la mise à jour du présent guide d'élaboration de politique de sécurité des systèmes d'information (PSSI), qui propose une démarche pour élaborer des PSSI et présente un catalogue de principes de sécurité permettant de rédiger des règles de sécurité selon le contexte ; ce guide est compatible avec les nouvelles lignes directrices (l'ancien reposait sur les lignes directrices de 1992) ;
- la diffusion de la méthode d'analyse des risques EBIOS (expression des besoins et d'identification des objectifs de sécurité), qui est largement diffusée et employée dans les secteurs publics et privés et pour laquelle des formations sont assurées par le centre de formation de la DCSSI :
    - elle contribue à la gestion des risques, l'un des principes des lignes directrices, et à la réévaluation des risques, un autre principe,

  - o les réflexions sur le processus continu de gestion des risques SSI sont compatibles avec les nouvelles lignes directrices ;
- la communication au sujet de la SSI sous la forme de sensibilisations, d'information, de formation, de mémentos ou de bonnes pratiques qui contribuent au principe de sensibilisation.

Sensibilisation des agents de l'État aux questions de sécurité

Le centre de formation à la sécurité des systèmes d'information (CFSSI), créé en 1986 et rattaché à la DCSSI, est l'acteur central d'un réseau de sensibilisation aux problèmes de la sécurité des systèmes d'information et le lieu de formation d'experts hautement qualifiés aux différents métiers de la discipline.

Le CFSSI propose des stages allant de la journée de sensibilisation à deux ans pour la préparation d'un brevet d'études supérieures de la sécurité des systèmes d'information. Les stages et journées de sensibilisation sont réservées à la formation et à l'information des agents de l'État dont les fonctions justifient cette formation.

2.2 Lignes directrices régissant la politique de cryptographie

Les lignes directrices régissant la politique de cryptographie ont été adoptées le 27 mars 1997 par le conseil de l'OCDE.

Elles ont notamment pour but de :

- promouvoir l'utilisation de la cryptographie (de manière à favoriser la confiance dans les infrastructures réseaux et systèmes d'information et contribuer à assurer la sécurité des données et protéger la vie privée),
- promouvoir l'utilisation de la cryptographie sans mettre en péril la sécurité publique, le respect des lois et la sécurité nationale,
- faire prendre conscience du besoin de politique et législation en matière de cryptographie,
- aider les décideurs des secteurs public et privé à élaborer et mettre en œuvre des politiques, méthodes et procédures cohérentes,
- promouvoir la coopération internationale pour parvenir à une utilisation concertée des méthodes cryptographiques.

Ces lignes directrices se présentent sous la forme des principes résumés ci-après.

Principe de confiance dans les méthodes cryptographiques

Les méthodes cryptographiques devraient susciter la confiance afin que les utilisateurs puissent se fier aux systèmes d'information et de communication.

Principe de choix des méthodes cryptographiques

Les utilisateurs devraient avoir le droit de choisir toute méthode cryptographique dans le respect de la législation applicable.

Principe de développement des méthodes cryptographiques guidé par le marché

Les méthodes cryptographiques devraient être développées en réponse aux besoins, aux demandes et aux responsabilités des personnes, des entreprises et des gouvernants.

Principe de normes applicables aux méthodes cryptographiques

Des normes, critères et protocoles techniques applicables aux méthodes cryptographiques devraient être élaborés et instaurés aux échelons national et international.

Principe de protection de la vie privée et des données à caractère personnel

Les droits fondamentaux des individus au respect de leur vie privée, notamment au secret des communications et à la protection des données à caractère personnel, devraient être respectées dans les politiques nationales à l'égard de la cryptographie et dans la mise en œuvre et l'utilisation des méthodes cryptographiques.

Principe d'accès légal

Les politiques nationales à l'égard de la cryptographie peuvent autoriser l'accès légal au texte en clair ou aux clés cryptographiques de données chiffrées. Ces politiques doivent respecter dans toute la mesure du possible les autres risques énoncés dans les lignes directrices.

Principe de responsabilité

Qu'elle soit établie par contrat ou par voie législative, la responsabilité des personnes et entités qui proposent des services cryptographiques ou détiennent des clés cryptographiques ou y ont accès, devrait clairement être énoncée.

Principe de coopération internationale

Les gouvernements devraient coopérer en vue de coordonner les politiques à l'égard de la cryptographie. Dans le cadre de cet effort, les gouvernements devraient veiller à la levée, ou éviter de créer au nom de la politique de cryptographie, des obstacles injustifiés aux échanges.

3 Codes d'éthique des métiers des technologies de l'information

3.1 Codes d'éthiques nationaux

Association Française des Informaticiens (AFIN)
Un code d'éthique, élaboré par l'Association française des informaticiens, est destiné à guider l'informaticien sur ses devoirs et droits. Le texte du code peut être adjoint aux contrats de travail et fait référence devant le Conseil des prud'hommes. Le texte s'articule autour de quatre grands chapitres :
- informaticiens et entreprise,
- entreprise et informaticiens,
- informaticien prestataire,
- informaticien vis-à-vis de ses confrères.

CLUb de la Sécurité des systèmes d'Information Français (CLUSIF)
Code d'éthique des métiers de la sécurité informatique, 1991.
Ce code[1] s'adresse en priorité aux membres du CLUSIF qui doivent s'y conformer sous peine d'exclusion.
Il est recommandé à tous les professionnels ou utilisateurs de l'informatique.
Le code du CLUSIF aborde les principes d'éthique selon les aspects suivants :
- règles générales,
- partie applicable aux consultants, niveau schéma directeur de la sécurité des systèmes d'information,
- partie applicable aux intervenants, niveau conception détaillée,
- partie applicable aux intervenants, niveau réalisation,
- partie applicable aux intervenants, niveau contrôle,
- partie applicable aux intervenants, niveau maintenance.

3.2 Autres codes d'éthique dans le monde

American Society for Information Science (ASIS)
Code of Ethics for Information Professionals, 1992
Ce code[2] s'applique aux membres de l'ASIS, il aborde les domaines suivants :
- responsabilité envers les employeurs, les clients et les utilisateurs,
- responsabilité envers la profession,
- responsabilité envers la société.

Association for Computing Machinery (ACM)
Code of Professionnal Conduct, 1972
Ce code[3] présente des principes généraux, chacun étant décliné sous l'aspect de l'éthique professionnelle et sous formes de règles à appliquer.
Les principes généraux s'adressent à tout membre de l'ACM et sont les suivants :
- l'intégrité,
- la compétence professionnelle,
- la responsabilité professionnelle,
- l'utilisation de ses compétences pour l'amélioration du bien-être de l'humanité.

[1] http://www.clusif.asso.fr/fr/clusif/adhesion/pdf/ethique_metier.pdf
[2] http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/ASIS.Code.html
[3] http://info.acm.org/constitution/code.html

British Computer Society (BCS)
Code of Conduct, 1990
Ce code[4] s'adresse aux membres de la BCS.
Les principes de base du code concernent :
- la conduite professionnelle,
- l'intégrité professionnelle,
- la préservation de l'intérêt public et du droit des tiers,
- la fidélité à l'employeur ou au client et le respect de la confidentialité des informations de l'employeur ou du client,
- la compétence technique,
- l'impartialité.

Canadian Information Processing Society (CIPS)
Code of Ethics and Professional Conduct, 1985
Ce code[5] canadien identifie les situations que les professionnels du traitement de l'information peuvent rencontrer et fournit des conseils pour y faire face.
Il est découpé en 4 sections :
- impératifs moraux généraux,
- responsabilités professionnelles plus spécifiques,
- impératifs relatifs aux dirigeants,
- respect du code.

Computer Professionals for Social Responsibility (CPSR) and Privacy International (PI)
Code of Fair Information Practices to promote information privacy, 1994
Les thèmes abordés dans ce code[6] concernent les données sur les personnes :
- ne pas utiliser de données personnelles dans un autre but que celui initialement prévu sans consentement spécifique,
- ne collecter que l'information nécessaire,
- assurer l'intégrité des données,
- informer les sujets de la mémorisation et de l'usage des informations qui les concernent, leur donner le droit de vérification et de correction,
- établir et diffuser la politique relative à la protection de la vie privée.

Institute of Electrical and Electronics Engineers (IEEE)
Ce code[7] de 1995 traite les thèmes suivants :
- accepter la responsabilité de prendre des décisions techniques en accord avec la sécurité, la santé et le bien-être du public, et dévoiler rapidement les facteurs qui pourraient mettre en danger le public ou l'environnement,
- éviter les conflits d'intérêts réels ou perçus, et les signaler aux parties concernées lorsqu'ils existent,
- être honnêtes et réalistes dans l'établissement d'affirmations ou d'estimations, basées sur des données existantes,
- refuser la corruption sous toutes ses formes,
- améliorer la compréhension de la technique, de son utilisation appropriée, et de ses conséquences potentielles,
- maintenir et améliorer la compétence technique et n'entreprendre un travail technique pour d'autres que si l'on est, par son éducation et son expérience, qualifié pour le faire ou après avoir expliqué complètement les limites de cette entreprise,
- rechercher, accepter et offrir des critiques honnêtes de travaux techniques, reconnaître et corriger ses erreurs, et mentionner correctement les contributions des autres,
- traiter justement toute personne, indépendamment de facteurs tels que la religion, le genre, la couleur de peau, l'infirmité, l'âge ou la nationalité,

4 http://ww1.bcs.org.uk/portal/showSection.asp?contentid=3224&link=/DocsRepository/03200/3224/default.htm

5 http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/Canada.Code.html

6 http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/CPRS.Code.html

7 http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/IEEE.Code.html

- éviter de porter préjudice à d'autres, à leur propriété, leur réputation ou leur emploi par des actions malhonnêtes ou malveillantes,
- assister ses collègues dans leur développement professionnel et les aider à suivre ce code d'éthique.

International Federation for Information Processing (IFIP)

Un code[8] d'éthique a été élaboré par l'IFIP (International Federation for Information Processing) dont l'ASTI (Association française des sciences et technologies de l'information) est membre, pour la France.
Ce code s'adresse non seulement aux professionnels de l'informatique mais encore aux organisations multinationales de l'informatique et à tous ceux qui se sentent concernés par les problèmes juridiques internationaux de l'informatique et par les règles publiques en ce domaine.
Le code est constitué des rubriques suivantes:

- éthique professionnelle des personnes,
- éthique des organisations internationales,
- éthique pour la législation internationale,
- éthique pour la politique internationale.

The Sytem Administrators Guild (SAGE)

Ce code[9] australien, destiné aux administrateurs système, aborde les thèmes suivants :

- l'intégrité d'un administrateur de système doit être au-dessus de tout reproche,
- un administrateur de système ne doit pas inutilement empiéter sur les droits des usagers,
- les contacts entre les administrateurs de système et les gens qu'ils fréquentent doivent respecter les plus hauts standards de comportement professionnel,
- la progression continuelle de l'éducation professionnelle est critique au maintien des qualifications d'un administrateur de système,
- un administrateur de système doit démontrer une éthique de travail exemplaire,
- en tout temps l'administrateur de système doit afficher son professionnalisme dans l'application de ses activités.

[8] *IFIP Code of Ethics, Revision of the preliminary IFIP Code of Ethics (1990)*. Unpublished Draft. Harold Sackman, California State University, Los Angeles, CA. Voir aussi la recommandation de l'IFIP relative aux codes de conduite à l'adresse http://courses.cs.vt.edu/~cs3604/lib/WorldCodes/IFIP.Recommendation.html.

[9] http://www.sage-au.org.au/ethics.html

4 Les atteintes aux personnes

4.1 La protection de la vie privée

Articles 226-1 à 226-8 du Code pénal

Articles R 226-1 à R 226-12 du Code pénal

Article 9 du Code civil

4.2 La protection du secret professionnel

Articles 226-13, 226-14 du Code pénal

Loi n°83-634 du 13 juillet 1983
Portant droits et obligations des fonctionnaires

4.3 La protection du secret de la correspondance

Articles 226-15, 432-9 du Code pénal

Loi n°86-1067 du 30 septembre 1986
Relative à la liberté de communication

Circulaire du 17 février 1988
Prise en application de l'article 43 de la loi 86-1067 du 30 septembre 1986 relative à la liberté de communication, concernant le régime déclaratif applicable à certains services de communication audiovisuelle

Loi n°91-646 du 10 juillet 1991
Relative au secret des correspondances émises par voie de télécommunications

4.4 La protection des données nominatives

Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 du Conseil de l'Europe (Convention 108)[10]

Directive générale n°95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil
Relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

Directive n°2002/58/CE du 12 juillet 2002 du Parlement européen et du Conseil
Relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

Directive sectorielle n°97/66/CE du 15 décembre 1997 du Parlement européen et du Conseil
Relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications

[10] http://conventions.coe.int

Loi n°78-17 du 6 janvier 1978
Relative à l'informatique, aux fichiers et aux libertés

Articles 226-16 à 226-24 du Code pénal (articles 41 et suivants de la loi)

Décret n°81-1142 du 23 décembre 1981
Instituant des contraventions de police en cas de violation de certaines dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifié par décret n°93-726 du 29 mars 1993)

Décret n°78-774 du 17 juillet 1978
Décret d'application de la loi

Décret n°79-1160 du 28 décembre 1979
Relatif aux traitements intéressant la sûreté de l'État

Rapports, recommandations et normes simplifiées de la CNIL[11]

[11] http://www.cnil.fr

5 Les atteintes aux biens

5.1 Le vol

Articles 311-1 et suivants du Code pénal

5.2 L'escroquerie

Articles 313-1 et suivants du Code pénal

5.3 Les détournements

Articles 314-1 et suivants du Code pénal

5.4 Les destructions, dégradations et détériorations

Articles 322-1 et suivants du Code pénal

5.5 Les atteintes aux systèmes d'informations

Articles 323-1 à 323-7 du Code pénal (issus de la loi n°88-19 du 5 janvier 1988)
Relatifs aux atteintes aux systèmes de traitement automatisés de données

6 Les atteintes aux intérêts fondamentaux de la nation, terrorisme et atteintes à la confiance publique

6.1 L'intelligence avec une puissance étrangère

Articles 411-4, 411-5 du Code pénal

6.2 La livraison d'informations à une puissance étrangère

Articles 411-6 à 411-8 du Code pénal

6.3 Le sabotage

Article 411-9 du Code pénal

6.4 Les atteintes au secret de la défense nationale

Articles 413-9 à 413-12 du Code pénal
Relatifs aux atteintes au secret de la défense nationale

Article R 413-6 du Code pénal

Décret 98-608 du 17 juillet 1998
Relatif à la protection des secrets de la défense nationale

Loi 98-567 du 8 juillet 1998
Loi instituant une Commission consultative du secret de la défense nationale

Instruction Générale Interministérielle n°1300/SGDN/PSE/SSD/DR
Sur la protection du secret de la défense nationale

Instruction Générale Interministérielle n°900/SGDN/SSD/DR
Relative à la sécurité des systèmes d'information faisant l'objet d'une classification de défense pour eux-même ou pour les informations traitées

6.5 Le terrorisme (atteintes aux systèmes de traitement automatisé de données)

Article 421-1, 2° Code pénal

6.6 Faux et usages de faux

Article 441-1 et suivants du Code pénal

7 Les atteintes à la propriété intellectuelle

7.1 La protection du droit d'auteur

Code de la propriété intellectuelle

Procédures et sanctions du C.P.I
Articles L. 331-1 et suivants

Directive n°91-250 du 14 mai 1991
Concernant la protection juridique des programmes d'ordinateur

Directive n°93/98 du 29 octobre 1993
Relative à l'harmonisation de la durée de protection du droit d'auteur et de certains droits voisins

Loi n°85-660 du 3 juillet 1985
Relative aux droits d'auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communications audiovisuelle.

Loi n°94-361 du 10 mai 1994
Portant mise en œuvre de la directive n°91-250 du Conseil des communautés européennes en date du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur et modifiant le code de la propriété intellectuelle

7.2 La protection des bases de données

Code de la propriété intellectuelle

Directive n°96/9/CE du 11 mars 1996 du Parlement européen
Concernant la protection juridique des bases de données

Loi n°98-536 du 1er juillet 1998
Portant transposition dans le Code de la propriété intellectuelle de la directive n°96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données

Article L. 341-1 et suivants du Code de la propriété intellectuelle
Relatifs aux droits des producteurs de bases de données

8 Les dispositions relatives à la cryptologie

Loi n°90-1170 du 29 décembre 1990 modifiée par la loi n°91-648 du 11 juillet 1991
Article 28

Loi n°96-659 du 26 juillet 1996

Décret n°98-101 du 24 février 1998
définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie

Décret n°98-102 du 24 février 1998
définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'Article 28 de la loi n°90-1170 du 29 décembre 1990 sur la réglementation des télécommunications

Décret n°99-199 du 17 mars 1999
définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation

Décret n°99-200 du 17 mars 1999
définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable

Règlement n°1334/2000 du Conseil du 22 juin 2000
Instituant un régime communautaire de contrôle des exportations de biens et technologies à double usage

Décret n°2001-1192 du 13 décembre 2001
Relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage

Loi n°2001-1062 du 15 novembre 2001
Relative à la sécurité quotidienne (Article 30 et 31)

Décret 2002-997 du 16 juillet 2002
Relatif à l'obligation mise à charge des fournisseurs de prestations de cryptologie en application de l'article 11-1 de la loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

Décret n°2002-1073 du 7 août 2002
D'application de l'article 30 de la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance

9 Les dispositions relatives à la signature électronique

Loi n°2000-230 du 13 mars 2000
portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Décret n°2001-272 du 30 mars 2001
pris pour application de l'art 1316-4 du code civil et relatif à la signature électronique.

Décret n°2002-535 du 18 avril 2002
relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Arrêté du 31 mai 2002
relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.

10 Autres textes

10.1 Au niveau national

10.1.1 Protection des intérêts économiques

Loi 68-678 du 26 juillet 1968 modifiée par la loi 80-538 du 16 juillet 1980
Loi relative à la communication de documents et de renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

Décret n°81-550 du 12 mai 1981
Portant application de l'article 2 de la loi n°68-678 du 26 juillet relative à la communication de documents et renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères.

10.1.2 Protection du secret

Instruction Interministérielle n°300/SGDN/TTS/SSI/DR du 21 juin 1997
relative à la protection contre les signaux parasites compromettants.

Guide n°400 SGDN/DISSI/SCSSI du 18 octobre 1991
relatif à l'installation des sites et systèmes traitant des informations sensibles ne relevant pas du secret de défense : protection contre les signaux parasites compromettants.

Guide n°430 DCSSI du 1er juin 1999
relatif à l'évaluation des équipements commerciaux au sens du zonage TEMPEST.

Guide n°460 SCSSI du 12 juin 1992
relatif au contrôle des sites et systèmes d'information - Protection contre les signaux compromettants.

Directive n°485 du 1er septembre 2000
relative aux règles d'installation des matériels ou systèmes d'information traitant des informations classifiées de défense.

Directive n°495 du 19 septembre 1997
relative au concept de zonage TEMPEST- Protection contre les signaux compromettants.

Directive n°520 du 15 janvier 1991
relative à l'emploi de la télécopie chiffrante.

Instruction interministérielle n°500bis/SGDN/TTS/SSI/DR du 18 octobre 1996
relative au chiffre dans la sécurité des systèmes d'information.

Instruction interministérielle n°910/SGDN/SSD/DR et n°910/SGDN/DISSI/SCSSI/DR du 19 décembre 1994
sur les articles contrôlés de la sécurité des systèmes d'information (ACSSI).

10.1.3 Systèmes d'information

Guide n°150 SCSSI du 10 février 1991
FEROS : Fiche d'expression rationnelle des objectifs de sécurité des systèmes d'information.

Recommandation n°600 de mars 1993
relatif à la protection des informations sensibles ne relevant pas du Secret de Défense : recommandations pour les postes de travail informatiques.

Guide n°650/DISSI/SCSSI du 28 mars 1994
relatif à la menace et aux attaques informatiques.

Recommandation n°901/DISSI/SCSSI du 2 mars 1994
relative à la sécurité des systèmes d'information traitant des informations sensibles non classifiées de défense.

Note de service n°63e SGDN/SCSSI/SI/bc du 2 mai 2000
note du Service central de la sécurité des systèmes d'information au sujet de la protection des informations et systèmes sensibles dans les administrations.

Directive 4201/SG du 13 avril 1995
Objectifs et organisation de la sécurité des systèmes d'information au sein des services de l'État.

10.1.4 Savoir-faire

Article L. 621-1 du Code de la propriété intellectuelle
Relatif au secret de fabrique.

Règlement CE n°240-96 du 31 janvier 1996
Concernant l'application de l'article 81 paragraphe 3 du traité à des catégories d'accords de transfert de technologie.

10.1.5 Cybersurveillance

La cybersurveillance des salariés dans l'entreprise
Rapport d'étude et de consultation publique de la CNIL.

Rapport de la CNIL sur la cybersurveillance sur les lieux de travail
adopté le 5 février 2002.

10.1.6 Autres

Circulaire du 18 janvier 1994
Commentaire des dispositions de la partie Réglementaire du nouveau Code pénal et des modifications de nature réglementaire nécessitées par son entrée en vigueur

Internet et réseaux numériques
Rapport du Conseil d'État

Loi n°78-753 du 17 juillet 1978, Article 6
relatif au droit d'accès aux documents administratifs et portant sur diverses mesures d'améliorations des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

Loi n°79-18 du 3 janvier 1979 modifiée par la loi 2000-321 du 12 avril 2000
relative aux archives.

10.2 Au niveau international

10.2.1 Conseil de l'Europe

Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999
relative au cadre communautaire pour les signatures électroniques.

Convention contre la « cybercriminalité » du 8 novembre 2001 du Conseil de l'Europe[12]

Résolutions et Recommandations du conseil de l'Europe
- Recommandation R (99) 5 sur la protection de la vie privée sur Internet (23 février 1999).
- Recommandation R (97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins statistiques (30 septembre 1997).
- Recommandation R (97) 5 sur la protection des données médicales (13 février 1997).
- Recommandation R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques (7 février 1995).
- Recommandation R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (9 septembre 1991).
- Recommandation R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes (13 septembre 1990).
- Recommandation R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi (18 janvier 1989).
- Recommandation R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987) et deuxième rapport d'évaluation (1998).
- Recommandation R (86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale (23 janvier 1986).
- Recommandation R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct (25 octobre 1985).
- Recommandation R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques (23 septembre 1983).
- Recommandation R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées (23 janvier 1981).
- Résolution (74) 29 sur la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs publics.
- Résolutions (73) 22 sur la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs privés.
- Recommandation du Conseil de l'Europe adoptée par le Conseil des ministres le 19 septembre 1989 relative à la criminalité en relation avec l'ordinateur.

10.2.2 ONU

Principes directeurs de l'ONU pour la réglementation des fichiers informatisés contenant des données à caractère personnel
adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990.
- Principes concernant les garanties minimales qui devraient être prévues dans les législations nationales.
- Application des principes directeurs aux fichiers contenant des données à caractère personnel, détenus par les organisations internationales gouvernementales.

[12] http://conventions.coe.int

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution