

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information

VERS UNE CULTURE DE LA SÉCURITÉ



ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

En vertu de l'article 1^{er} de la Convention signée le 14 décembre 1960, à Paris, et entrée en vigueur le 30 septembre 1961, l'Organisation de Coopération et de Développement Économiques (OCDE) a pour objectif de promouvoir des politiques visant :

- À réaliser la plus forte expansion de l'économie de l'emploi et une progression du niveau de vie dans les pays Membres, tout en maintenant la stabilité financière, et à contribuer ainsi au développement de l'économie mondiale.
- À contribuer à une saine expansion économique dans les pays Membres ainsi que les pays non membres, en voie de développement économique.
- À contribuer à l'expansion du commerce mondial sur une base multilatérale et non discriminatoire conformément aux obligations internationales.

Les pays Membres originaires de l'OCDE sont : l'Allemagne, l'Autriche, la Belgique, le Canada, le Danemark, l'Espagne, les États-Unis, la France, la Grèce, l'Irlande, l'Islande, l'Italie, le Luxembourg, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède, la Suisse et la Turquie. Les pays suivants sont ultérieurement devenus Membres par adhésion aux dates indiquées ci-après : le Japon (28 avril 1964), la Finlande (28 janvier 1969), l'Australie (7 juin 1971), la Nouvelle-Zélande (29 mai 1973), le Mexique (18 mai 1994), la République tchèque (21 décembre 1995), la Hongrie (7 mai 1996), la Pologne (22 novembre 1996), la Corée (12 décembre 1996) et la République slovaque (14 décembre 2000). La Commission des Communautés européennes participe aux travaux de l'OCDE (article 13 de la Convention de l'OCDE).

Also available in English under the title:

**OECD Guidelines for the Security of Information Systems and Networks:
Towards a Culture of Security**

© OCDE 2002

Les permissions de reproduction partielle à usage non commercial ou destinée à une formation doivent être adressées au Centre français d'exploitation du droit de copie (CFC), 20, rue des Grands-Augustins, 75006 Paris, France, tél. (33-1) 44 07 47 70, fax (33-1) 46 34 67 19, pour tous les pays à l'exception des États-Unis. Aux États-Unis, l'autorisation doit être obtenue du Copyright Clearance Center, Customer Service, (508) 750-8400, 222 Rosewood Drive, Danvers, MA 01923 USA, ou CCC Online: www.copyright.com. Toute autre demande d'autorisation de reproduction ou de traduction totale ou partielle de cette publication doit être adressée aux Éditions de l'OCDE, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

AVANT-PROPOS

Les présentes *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* ont été adoptées sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037ème session, le 25 juillet 2002.

TABLE DES MATIÈRES

LES LIGNES DIRECTRICES RÉGISSANT LA SÉCURITÉ DES SYSTÈMES ET RÉSEAUX D'INFORMATION : <i>VERS UNE CULTURE DE LA SÉCURITÉ</i>	7
PRÉFACE.....	7
I. VERS UNE CULTURE DE LA SÉCURITÉ.....	8
II. BUTS.....	9
III. PRINCIPES	9
RECOMMANDATION DU CONSEIL	15
HISTORIQUE DE LA PROCÉDURE.....	18

LES LIGNES DIRECTRICES RÉGISSANT LA SÉCURITÉ DES SYSTÈMES ET RÉSEAUX D'INFORMATION

VERS UNE CULTURE DE LA SÉCURITÉ

PRÉFACE

Le degré d'utilisation des systèmes et réseaux d'information et l'environnement des technologies de l'information dans son ensemble ont évolué de façon spectaculaire depuis 1992, date à laquelle l'OCDE a rendu publiques ses *Lignes directrices régissant la sécurité des systèmes d'information*. Ces évolutions constantes offrent des avantages significatifs mais requièrent également que les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information (parties prenantes), portent une bien plus grande attention à la sécurité.

Des ordinateurs personnels toujours plus puissants, des technologies convergentes et la très large utilisation de l'Internet ont remplacé ce qui était autrefois des systèmes autonomes aux capacités limitées, dans des réseaux essentiellement fermés. Aujourd'hui, les parties prenantes sont de plus en plus interconnectées et les connexions franchissent les frontières nationales. De surcroît, l'Internet est le support d'infrastructures vitales telles que l'énergie, les transports et les activités financières et joue un rôle majeur dans la façon dont les entreprises conduisent leurs activités, dont les gouvernements assurent des services aux citoyens et aux entreprises et dont les citoyens communiquent et échangent des informations. La nature et le type des technologies constituant l'infrastructure des communications et de l'information ont également sensiblement évolué. Le nombre et la nature des dispositifs d'accès à cette infrastructure se sont multipliés et diversifiés pour englober les terminaux d'accès fixes, sans fil et mobiles et une proportion croissante des accès s'effectue par l'intermédiaire de connexions « permanentes ». Par voie de conséquence, la nature, le volume et le caractère sensible de l'information échangée ont augmenté de façon significative.

Du fait de leur connectivité croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre croissant et à un éventail plus large de menaces et vulnérabilités, ce qui pose de nouveaux problèmes de sécurité. Les présentes Lignes directrices s'adressent donc à l'ensemble des parties prenantes à la nouvelle société de l'information, et suggèrent le besoin d'une prise de

conscience et d'une compréhension des questions de sécurité accrues, ainsi que la nécessité de développer une « culture de la sécurité ».

I. VERS UNE CULTURE DE LA SÉCURITÉ

Ces Lignes directrices répondent à un environnement en constante évolution en appelant au développement d'une culture de la sécurité – ce qui signifie porter une attention très grande à la sécurité lors du développement des systèmes d'information et des réseaux et adopter de nouveaux modes de pensée et de comportement lors de l'utilisation des systèmes et réseaux d'information et dans le cadre des échanges qui y prennent place. Les Lignes directrices marquent une rupture nette avec un temps où la sécurité n'intervenait que trop souvent de façon incidente dans la conception et l'utilisation des réseaux et systèmes d'information. Les parties prenantes sont de plus en plus tributaires des systèmes d'information, des réseaux et des services qui leur sont liés, lesquels doivent tous être fiables et sécurisés. Seule une approche prenant dûment en compte les intérêts de toutes les parties prenantes et la nature des systèmes, réseaux et services connexes peut permettre d'assurer une sécurité efficace.

Chaque partie prenante a un rôle important à jouer pour assurer la sécurité. Les parties prenantes, en fonction de leurs rôles respectifs, doivent être sensibilisées aux risques liés à la sécurité ainsi qu'aux parades appropriées, doivent assumer leurs responsabilités et prendre des mesures de nature à améliorer la sécurité des systèmes et réseaux d'information.

L'instauration d'une culture de la sécurité nécessitera à la fois une impulsion et une large participation et devrait se traduire par une priorité renforcée donnée à la planification et la gestion de la sécurité, ainsi que par une compréhension de l'exigence de sécurité par l'ensemble des participants. Les questions de sécurité doivent être un sujet de préoccupation et de responsabilité à tous les niveaux du gouvernement et des entreprises et pour l'ensemble des parties prenantes. Les présentes Lignes directrices offrent un fondement aux efforts en vue d'instaurer une culture de la sécurité dans l'ensemble de la société. Les parties prenantes seront ainsi à même d'agir pour que la sécurité devienne partie intégrante de la conception et de l'utilisation de tous les systèmes et réseaux d'information. Les Lignes directrices proposent que toutes les parties prenantes adoptent et encouragent une « culture de la sécurité » qui guide la réflexion, la décision et l'action concernant le fonctionnement des systèmes et réseaux d'information.

II. BUTS

L'objet des Lignes directrices est de :

- Promouvoir parmi l'ensemble des parties prenantes une culture de la sécurité en tant que moyen de protection des systèmes et réseaux d'information.
- Renforcer la sensibilisation aux risques pour les systèmes et réseaux d'information, aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, ainsi qu'à la nécessité de les adopter et de les mettre en œuvre.
- Promouvoir parmi l'ensemble des parties prenantes une plus grande confiance dans les systèmes et réseaux d'information et dans la manière dont ceux-ci sont mis à disposition et utilisés.
- Créer un cadre général de référence qui aide les parties prenantes à comprendre la nature des problèmes liés à la sécurité, et à respecter les valeurs éthiques dans l'élaboration et la mise en œuvre de politiques, pratiques, mesures et procédures cohérentes pour la sécurité des systèmes et réseaux d'information.
- Promouvoir parmi l'ensemble des parties prenantes, la coopération et le partage d'informations appropriés pour l'élaboration et la mise en œuvre des politiques, pratiques, mesures et procédures pour la sécurité.
- Promouvoir la prise en considération de la sécurité en tant qu'objectif important parmi toutes les parties prenantes associées à l'élaboration et la mise en œuvre de normes.

III. PRINCIPES

Les neuf principes exposés ci-après se complètent et doivent être considérés comme un tout. Ils s'adressent aux parties prenantes à tous les niveaux, y compris politique et opérationnel. Aux termes des Lignes directrices, les responsabilités des parties prenantes varient selon le rôle qui est le leur. Toutes les parties prenantes, peuvent être aidées par des actions de sensibilisation, d'éducation, de partage d'informations et de formation de nature à faciliter une meilleure compréhension des questions de sécurité et l'adoption de meilleures pratiques en ce domaine. Les efforts visant à renforcer la sécurité des systèmes et réseaux d'information doivent respecter les valeurs d'une société

démocratique, en particulier le besoin d'une circulation libre et ouverte de l'information ainsi que les principes de base de respect de la vie privée des individus.¹

1) 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.

La sensibilisation aux risques et aux parades disponibles est la première ligne de défense pour assurer la sécurité des systèmes et réseaux d'information. Les systèmes et réseaux d'information peuvent être exposés à des risques tant internes qu'externes. Les parties prenantes doivent comprendre que les défaillances de sécurité peuvent gravement porter atteinte aux systèmes et réseaux sous leur contrôle mais aussi, du fait de l'interconnectivité et de l'interdépendance, à ceux d'autrui. Les parties prenantes doivent réfléchir à la configuration de leur système, aux mises à jour disponibles pour ce dernier, à la place qu'il occupe dans les réseaux, aux bonnes pratiques qu'elles peuvent mettre en œuvre pour renforcer la sécurité, ainsi qu'aux besoins des autres parties prenantes.

2) Responsabilité

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

Les parties prenantes sont tributaires de systèmes et réseaux d'information locaux et mondiaux interconnectés. Elles doivent comprendre leur responsabilité dans la sécurité de ces systèmes et réseaux et en être, en fonction du rôle qui est le leur, individuellement comptables. Elles doivent régulièrement examiner et évaluer leurs propres politiques, pratiques, mesures et procédures pour s'assurer qu'elles sont adaptées à leur environnement. Celles qui développent, conçoivent et fournissent des produits et services doivent prendre en compte la sécurité des systèmes et

1. Outre les présentes Lignes directrices sur la sécurité, l'OCDE a élaboré une série de recommandations complémentaires concernant des lignes directrices relatives à d'autres aspects importants de la société mondiale de l'information. Celles-ci visent la vie privée (*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, 1980) et la cryptographie (*Lignes directrices régissant la politique de cryptographie*, OCDE, 1997). Les présentes Lignes directrices sur la sécurité doivent être lues en parallèle avec ces autres Lignes directrices.

réseaux et diffuser des informations appropriées, notamment des mises à jour en temps opportun de manière à ce que les utilisateurs puissent mieux comprendre les fonctions de sécurité des produits et services et leurs responsabilités en la matière.

3) Réaction

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

Du fait de l'interconnectivité des systèmes et réseaux d'information et de la propension des dommages à se répandre rapidement et massivement, les parties prenantes doivent réagir avec promptitude et dans un esprit de coopération aux incidents de sécurité. Elles doivent échanger leurs informations sur les menaces et vulnérabilités de manière appropriée et mettre en place des procédures pour une coopération rapide et efficace afin de prévenir et détecter les incidents de sécurité et y répondre. Lorsque cela est autorisé, cela peut impliquer des échanges d'informations et une coopération transfrontières.

4) Éthique

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

Les systèmes et réseaux d'information sont omniprésents dans nos sociétés et les parties prenantes doivent être conscientes du tort qu'elles peuvent causer à autrui par leur action ou leur inaction. Une conduite éthique est donc indispensable et les parties prenantes doivent s'efforcer d'élaborer et d'adopter des pratiques exemplaires et de promouvoir des comportements qui tiennent compte des impératifs de sécurité et respectent les intérêts légitimes des autres parties prenantes.

5) Démocratie

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

La sécurité doit être assurée dans le respect des valeurs reconnues par les sociétés démocratiques, et notamment la liberté d'échanger des pensées et des idées, la libre circulation de l'information, la confidentialité de l'information et des communications, la protection adéquate des informations de caractère personnel, l'ouverture et la transparence.

6) *Évaluation des risques*

Les parties prenantes doivent procéder à des évaluations des risques.

L'évaluation des risques permet de déceler les menaces et vulnérabilités et doit être suffisamment large pour couvrir l'ensemble des principaux facteurs internes et externes, tels la technologie, les facteurs physiques et humains, les politiques et services de tierces parties ayant des implications sur la sécurité. L'évaluation des risques permettra de déterminer le niveau acceptable de risque et facilitera la sélection de mesures de contrôles appropriées pour gérer le risque de préjudices possibles pour les systèmes et réseaux d'information compte tenu de la nature et de l'importance de l'information à protéger. L'évaluation des risques doit tenir compte des préjudices aux intérêts d'autrui ou causés par autrui rendus possibles par l'interconnexion croissante des systèmes d'information.

7) *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.

Les systèmes, réseaux et politiques doivent être conçus, mis en œuvre et coordonnés de façon appropriée afin d'optimiser la sécurité. Un axe majeur, mais non exclusif, de cet effort doit être la conception et l'adoption de mesures de protection et solutions appropriées afin de prévenir ou limiter les préjudices possibles liés aux vulnérabilités et menaces identifiées. Les mesures de protection et solutions doivent être à la fois techniques et non techniques et être proportionnées à la valeur de l'information dans les systèmes et réseaux d'information de l'organisation. La sécurité doit être un élément fondamental de l'ensemble des produits, services, systèmes et réseaux et faire partie intégrante de la conception et de l'architecture des systèmes. Pour l'utilisateur final, la conception et la mise en œuvre de la sécurité consistent essentiellement à sélectionner et configurer des produits et services pour leurs systèmes.

8) *Gestion de la sécurité*

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

La gestion de la sécurité doit être fondée sur l'évaluation des risques et être dynamique et globale afin de couvrir tous les niveaux d'activités des parties prenantes et tous les aspects de leurs opérations. Elle doit inclure également, par anticipation, des réponses aux menaces émergentes et couvrir la

prévention, la détection et la résolution des incidents, la reprise des systèmes, la maintenance permanente, le contrôle et l'audit. Les politiques de sécurité des systèmes et réseaux d'information, les pratiques, mesures et procédures en matière de sécurité doivent être coordonnées et intégrées pour créer un système cohérent de sécurité. Les exigences de la gestion de la sécurité sont fonction du niveau de participation, du rôle de la partie prenante, des risques en jeu et des caractéristiques du système.

9) 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.

Des vulnérabilités et menaces nouvelles ou évolutives sont constamment découvertes. Toutes les parties prenantes doivent continuellement revoir, réévaluer et modifier tous les aspects de la sécurité pour faire face à ces risques évolutifs.

**RECOMMANDATION DU CONSEIL CONCERNANT
LES LIGNES DIRECTRICES RÉGISSANT LA SÉCURITÉ
DES SYSTÈMES ET RÉSEAUX D'INFORMATION**

VERS UNE CULTURE DE LA SÉCURITÉ

LE CONSEIL,

Vu la Convention relative à l'Organisation de Coopération et de Développement Économiques, en date du 14 décembre 1960, et notamment ses articles 1 b), 1 c), 3 a) et 5 b) ;

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, en date du 23 septembre 1980 [C(80)58(Final)] ;

Vu la Déclaration sur les flux transfrontières de données adoptée par les gouvernements des pays Membres de l'OCDE le 11 avril 1985 [C(85)139, Annexe] ;

Vu la Recommandation du Conseil relative aux Lignes directrices régissant la politique de cryptographie, en date du 27 mars 1997 [C(97)62/FINAL] ;

Vu la Déclaration ministérielle relative à la protection de la vie privée sur les réseaux mondiaux, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe] ;

Vu la Déclaration ministérielle sur l'authentification pour le commerce électronique, en date des 7-9 décembre 1998 [C(98)177/FINAL, Annexe] ;

Reconnaissant que les systèmes et réseaux d'information sont de plus en plus utilisés et acquièrent une valeur croissante pour les gouvernements, les entreprises, les autres organisations, et les utilisateurs individuels ;

Reconnaissant que le rôle toujours plus important que jouent les systèmes et réseaux d'information dans la stabilité et l'efficacité des économies nationales et des échanges internationaux, ainsi que dans la vie sociale, culturelle et politique, et l'accentuation de la dépendance à leur égard imposent

des efforts particuliers pour protéger et promouvoir la confiance qui les entoure ;

Reconnaissant que les systèmes et réseaux d'information et leur expansion à l'échelle mondiale se sont accompagnés de risques nouveaux et en nombre croissant ;

Reconnaissant que les données et informations conservées ou transmises sur des systèmes et réseaux d'information sont exposées à des menaces du fait de divers moyens d'accès sans autorisation, d'utilisation, d'appropriation abusive, d'altération, de transmission de code malveillant, de déni de service ou de destruction, et exigent des mesures de protection appropriées ;

Reconnaissant qu'il importe de sensibiliser davantage aux risques pesant sur les systèmes et réseaux d'information ainsi qu'aux politiques, pratiques, mesures et procédures disponibles pour faire face à ces risques, et d'encourager des comportements appropriés en ce qu'ils constituent une étape essentielle dans le développement d'une culture de la sécurité ;

Reconnaissant qu'il convient de revoir les politiques, pratiques, mesures et procédures actuelles pour aider à faire en sorte qu'elles répondent de façon adéquate aux défis en constante évolution que posent les menaces auxquelles sont exposés les systèmes et réseaux d'information ;

Reconnaissant qu'il est de l'intérêt commun de promouvoir la sécurité des systèmes et réseaux d'information par une culture de la sécurité qui encourage une coordination et une coopération internationales appropriées en vue de répondre aux défis posés par les préjudices que des défaillances de la sécurité sont susceptibles de causer aux économies nationales, aux échanges internationaux, ainsi qu'à la participation à la vie sociale, culturelle et politique.

Reconnaissant en outre que les *Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité*, figurant en annexe à la présente Recommandation, sont d'application volontaire et n'affectent pas les droits souverains des États ;

Et reconnaissant que l'objet de ces Lignes directrices n'est pas de suggérer qu'il existe une solution unique quelconque en matière de sécurité, ou que des politiques, pratiques, mesures et procédures particulières soient adaptées à une situation donnée, mais plutôt de fournir un cadre plus général de principes de nature à favoriser une meilleure compréhension de la manière dont

les parties prenantes peuvent à la fois bénéficier du développement d'une culture de la sécurité et y contribuer ;

PRÉCONISE l'application de ces *Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* par les gouvernements, les entreprises, les autres organisations et les utilisateurs individuels qui développent, possèdent, fournissent, gèrent, maintiennent et utilisent les systèmes et réseaux d'information ;

RECOMMANDE aux pays Membres :

D'établir de nouvelles politiques, pratiques, mesures et procédures ou de modifier celles qui existent pour refléter et prendre en compte les *Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* en adoptant et promouvant une culture de la sécurité, conformément auxdites Lignes directrices ;

D'engager des actions de consultation, de coordination et de coopération, aux plans national et international, pour la mise en œuvre des Lignes directrices ;

De diffuser les Lignes directrices dans l'ensemble des secteurs public et privé, notamment auprès des gouvernements, des entreprises, d'autres organisations et des utilisateurs individuels, pour promouvoir une culture de la sécurité, et encourager toutes les parties intéressées à adopter une attitude responsable et à prendre les mesures nécessaires en fonction des rôles qui sont les leurs ;

De mettre les Lignes directrices à la disposition des pays non membres, le plus rapidement possible et de manière appropriée ;

De réexaminer les Lignes directrices tous les cinq ans, de manière à promouvoir une coopération internationale sur les questions liées à la sécurité des systèmes et réseaux d'information ;

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de l'OCDE d'apporter son soutien à la mise en œuvre des Lignes directrices.

La présente Recommandation remplace la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes d'information du 26 novembre 1992 [C(92)188/FINAL].

HISTORIQUE DE LA PROCÉDURE

Les Lignes directrices sur la sécurité ont été achevées en 1992 puis réexaminées en 1997. L'examen actuel a été entrepris en 2001 par le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP), dans le cadre d'un mandat donné par le Comité de la politique de l'information, de l'informatique et des communications (PIIC), et accéléré suite à la tragédie du 11 septembre.

La rédaction a été entreprise par un Groupe d'experts du GTSIVP qui s'est réuni à Washington, DC, les 10 et 11 décembre 2001, à Sydney les 12-13 février 2002 et à Paris les 4 et 6 mars 2002. Le GTSIVP s'est réuni les 5-6 mars 2002, les 22-23 avril 2002 et les 25-26 juin 2002.

Les présentes *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* ont été adoptées sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037^{ème} session, le 25 juillet 2002.