OECD Guidelines for the Security of Information Systems and Networks

TOWARDS A CULTURE OF SECURITY

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

VERS UNE CULTURE DE LA SÉCURITÉ

OECD

OECD Guidelines for the Security of Information Systems and Networks:

Towards a Culture of Security

♦

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

vers une culture de la sécurité

OECD OCDE

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

En vertu de l'article 1er 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 et 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).

FOREWORD

The present *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.

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 OF CONTENTS

TABLE DES MATIÈRES

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

TOWARDS A CULTURE OF SECURITY

PREFACE

The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the *Guidelines for the Security of Information Systems*. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage service and use information systems and networks ("participants").

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".

I. TOWARDS A CULTURE OF SECURITY

These Guidelines respond to an ever changing security environment by promoting the development of a culture of security – that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often afterthoughts. Participants are becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks and related services, can provide effective security.

Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks.

Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants. These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

II. AIMS

These Guidelines aim to:

- Promote a culture of security among all participants as a means of protecting information systems and networks.
- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.

- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

III. PRINCIPLES

The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy.[1]

1. In addition to these Security Guidelines, the OECD has developed complementary recommendations concerning guidelines on other issues important to the world's information society. They relate to privacy (the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*) and cryptography (the 1997 *OECD Guidelines for Cryptography Policy*). These Security Guidelines should be read in conjunction with them.

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

Participants should respect the legitimate interests of others.

Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

TOWARDS A CULTURE OF SECURITY

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, Articles 1 b), 1 c), 3 a) and 5 b) thereof;

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];

Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];

Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];

Recognising that information systems and networks are of increasing use and value to governments, businesses, other organisations and individual users;

Recognising that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;

Recognising that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;

Recognising that data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;

Recognising that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;

Recognising that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;

Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;

And further recognising that the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;

And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;

COMMENDS these *Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security* to governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks;

RECOMMENDS that Member countries:

Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* by adopting and promoting a culture of security as set out in the Guidelines;

Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;

Disseminate the Guidelines throughout the public and private sectors, including to governments, business, other organisations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;

Make the Guidelines available to non-member countries in a timely and appropriate manner;

Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.

This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL].

PROCEDURAL HISTORY

The Security Guidelines were first completed in 1992 and were reviewed in 1997. The current review was undertaken in 2001 by the Working Party on Information Security and Privacy (WPISP), pursuant to a mandate from the Committee for Information, Computer and Communications Policy (ICCP), and accelerated in the aftermath of the September 11 tragedy.

Drafting was undertaken by an Expert Group of the WPISP which met in Washington, DC, on 10-11 December 2001, Sydney on 12-13 February 2002 and Paris on 4 and 6 March 2002. The WPISP met in Paris on 5-6 March 2002, 22-23 April 2002 and 25-26 June 2002.

The present *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.

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 REGISSANT LA SECURITÉ DES SYSTÈMES ET RÉSEAUX D'INFORMATION

VERS UNE CULTURE DE LA SECURITÉ

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'efficience 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 1037ème session, le 25 juillet 2002.

OECD PUBLICATIONS, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(00 2002 30 3 P) – No. 81829 2002