Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security

OECD Legal Instruments

OECD
BETTER POLICIES FOR BETTER LIVES

Please cite this document as:
OECD, *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security*, OECD/LEGAL/0312

Series: OECD Legal Instruments

Date(s)

Adopted on 25/07/2002
Abrogated on 17/09/2015

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].

ANNEX

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

TOWARDS A CULTURE OF SECURITY

Preface

1. 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").

2. 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.

3. 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

4. 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.

5. 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.

6. 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

7. 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

8. 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) 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.

---

[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.

Adherents*

OECD Members	Non-Members
Australia	
Austria	
Belgium	
Canada	
Chile	
Czech Republic	
Denmark	
Estonia	
Finland	
France	
Germany	
Greece	
Hungary	
Iceland	
Ireland	
Israel	
Italy	
Japan	
Korea	
Latvia	
Luxembourg	
Mexico	
Netherlands	
New Zealand	
Norway	
Poland	
Portugal	
Slovak Republic	
Slovenia	
Spain	
Sweden	
Switzerland	
Turkey	
United Kingdom	
United States	

*Additional information and statements are available in the Compendium of OECD Legal Instruments: http://legalinstruments.oecd.org

About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Legal Instruments

Since the creation of the OECD in 1961, around 450 substantive legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions**: OECD legal instruments which are legally binding on all Members except those which abstain at the time of adoption. While they are not international treaties, they entail the same kind of legal obligations. Adherents are obliged to implement Decisions and must take the measures necessary for such implementation.

- **Recommendations**: OECD legal instruments which are not legally binding but practice accords them great moral force as representing the political will of Adherents. There is an expectation that Adherents will do their utmost to fully implement a Recommendation. Thus, Members which do not intend to do so usually abstain when a Recommendation is adopted, although this is not required in legal terms.

- **Declarations**: OECD legal instruments which are prepared within the Organisation, generally within a subsidiary body. They usually set general principles or long-term goals, have a solemn character and are usually adopted at Ministerial meetings of the Council or of committees of the Organisation.

- **International Agreements**: OECD legal instruments negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangement, Understanding and Others**: several ad hoc substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.