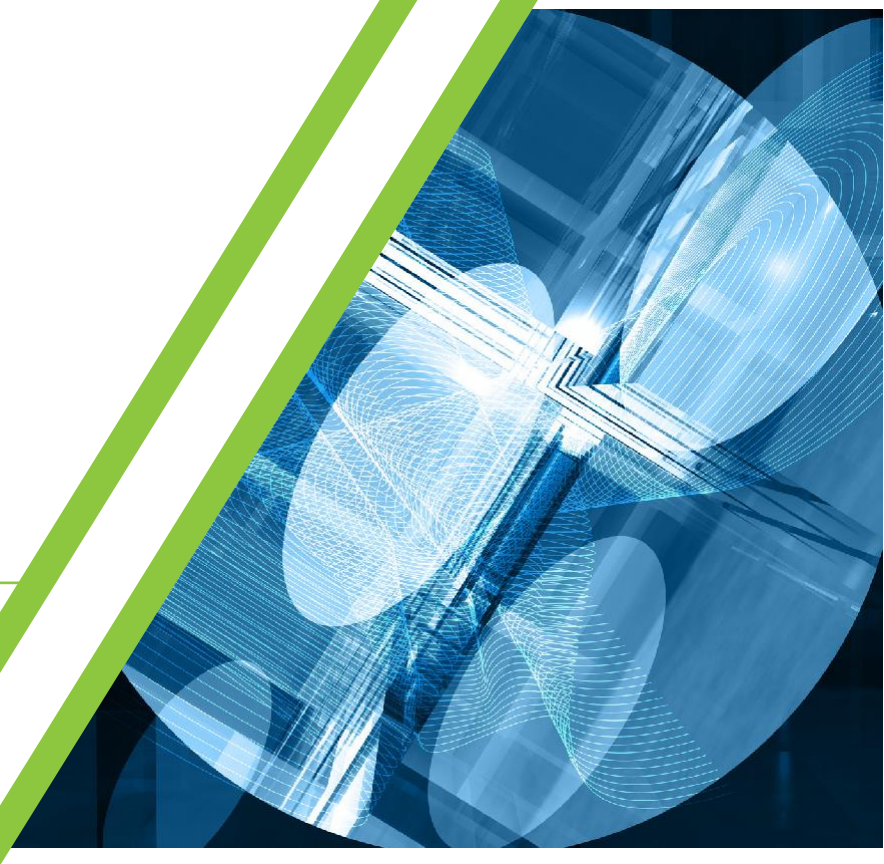
Recommendation of the Council concerning Guidelines for the Security of Information Systems



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*, OECD/LEGAL/0271

Series: OECD Legal Instruments

Background Information

THE COUNCIL,

HAVING REGARD TO:

1. 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;

2. 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)];

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

RECOGNISING:

1. the increasing use and value of computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance (all hereinafter referred to collectively as "information systems");

2. the international nature of information systems and their worldwide proliferation;

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

4. that, in the absence of appropriate safeguards, data and information in information systems acquire a distinct sensitivity and vulnerability, as compared with paper documents, due to risks arising from available means of unauthorised access, use, misappropriation, alteration, and destruction;

5. the need to raise awareness of risks to information systems and of the safeguards available to meet those risks;

6. that present measures, practices, procedures and institutions may not adequately meet the challenges posed by information systems and the concomitant need for clarity, predictability, certainty, and uniformity of rights and obligations, of enforcement of rights, and of recourse and redress for violation of rights relating to information systems and the security of information systems;

7. the desirability of greater international co-ordination and co-operation in meeting the challenges posed by information systems, the potential detrimental effects of a lack of co-ordination and co-operation on national and international economies and trade and on participation in social, cultural and political life, and the common interest in promoting the security of information systems;

AND FURTHER RECOGNISING:

1. that the Guidelines do not affect the sovereign rights of national governments in respect of national security and public order ("ordre public"), subject always to the requirements of national law;

2. that, in the particular case of federal countries, the observance of the Guidelines may be affected by the division of powers in the federation;

RECOMMENDS THAT MEMBER COUNTRIES:

1. establish measures, practices and procedures to reflect the principles concerning the security of information systems set forth in the Guidelines contained in the Appendix to this Recommendation, which is an integral part hereof;

2. consult, co-ordinate and co-operate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices and procedures for the security of information systems;

3. agree as expeditiously as possible on specific initiatives for the application of the Guidelines;

4. disseminate extensively the principles contained in the Guidelines;

5. review the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems.

APPENDIX

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

I. AIMS

The Guidelines are intended:

a) to raise awareness of risks to information systems and of the safeguards available to meet those risks;

b) to create a general framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems;

c) to promote co-operation between the public and private sectors in the development and implementation of such measures, practices and procedures;

d) to foster confidence in information systems and the manner in which they are provided and used;

e) to facilitate development and use of information systems, nationally and internationally; and

f) to promote international co-operation in achieving security of information systems.

II. SCOPE

The Guidelines are addressed to the public and private sectors.

The Guidelines apply to all information systems.

The Guidelines are capable of being supplemented by additional practices and procedures for the provision of the security of information systems.

III. DEFINITIONS

For the purposes of these Guidelines:

a) "data" means a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means;

b) "information" is the meaning assigned to data by means of conventions applied to that data;

c) "information systems" means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or

transmitted by them, including programs, specifications and procedures for their operation, use and maintenance;

d) "availability" means the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner;

e) "confidentiality" means the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner;

f) "integrity" means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

IV. SECURITY OBJECTIVE

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

V. PRINCIPLES

Accountability Principle

1. The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

Awareness Principle

2. In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

Ethics Principle

3. Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

Multidisciplinary Principle

4. Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

Proportionality Principle

5. Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

Integration Principle

6. Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

Timeliness Principle

7. Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

Reassessment Principle

8. The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

Democracy Principle

9. The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

VI. IMPLEMENTATION

Governments, the public sector and the private sector should take steps to protect information systems and to provide for their security in accordance with the Principles of the Guidelines. In achieving the Security Objective and in implementing the Principles, they are urged, as appropriate, to establish and to encourage and support the establishment of legal, administrative, self-regulatory and other measures, practices, procedures and institutions for the security of information systems. Where provision has not already been made, they should, in particular:

Policy Development

a) Adopt and encourage the adoption of appropriate policies, laws, decrees, rules, and international agreements, including provision for:

harmonized worldwide technical standards, methods and codes of practice;

promotion of expertise and best practice in the security of information systems;

formation and validity of contracts and other documents created and executed in or by means of information systems;

allocation of risks and liability for failures of the security of information systems;

penal, administrative or other sanctions for misuse of information systems;

jurisdictional competence of courts, including rules on extraterritorial jurisdiction, and administrative competence of other bodies;

mutual assistance, extradition and other international co-operation in matters relating to the security of information systems; and

means of obtaining evidence in information systems and the admissibility of such evidence in penal and non-penal legal and administrative proceedings.

Education and Training

b) Promote awareness of the necessity for and the goals of security of information systems, including:

ethical conduct in the use of information systems; and

adoption of good security practices.

c) Provide and foster education and training of:

developers, owners, providers and users of information systems;

specialists and auditors of information systems;

specialists and auditors of security of information systems; and

law enforcement authorities, investigators, attorneys and judges.

Enforcement and Redress

d) Provide accessible and adequate means for the exercise and enforcement of rights arising from the implementation of the Guidelines and for recourse and redress for violations of those rights.

e) Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.

Exchange of Information

f) Facilitate the exchange of information relating to the Guidelines and their implementation.

g) Publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems.

Co-operation

h) On national and international levels, consult, co-ordinate and co-operate between and among governments and the private sector to encourage implementation of the Guidelines and to harmonize as completely as possible measures, practices and procedures for the security of information systems.

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, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Türkiye, 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 460 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** are adopted by Council and are legally binding on all Members except those which abstain at the time of adoption. They set out specific rights and obligations and may contain monitoring mechanisms.

- **Recommendations** are adopted by Council and are not legally binding. They represent a political commitment to the principles they contain and entail an expectation that Adherents will do their best to implement them.

- **Substantive Outcome Documents** are adopted by the individual listed Adherents rather than by an OECD body, as the outcome of a ministerial, high-level or other meeting within the framework of the Organisation. They usually set general principles or long-term goals and have a solemn character.

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

- **Arrangement, Understanding and Others**: several other types of 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.