

INTERNATIONAL
STANDARD

ISO/IEC
17799

Second edition
2005-06-15

**Information technology — Security
techniques — Code of practice for
information security management**

*Technologies de l'information — Techniques de sécurité — Code de
pratique pour la gestion de sécurité d'information*

Reference number
ISO/IEC 17799:2005(E)



© ISO/IEC 2005

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents	Page
FOREWORD	VII
0 INTRODUCTION	VIII
0.1 WHAT IS INFORMATION SECURITY?.....	VIII
0.2 WHY INFORMATION SECURITY IS NEEDED?	VIII
0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS	IX
0.4 ASSESSING SECURITY RISKS	IX
0.5 SELECTING CONTROLS.....	IX
0.6 INFORMATION SECURITY STARTING POINT.....	IX
0.7 CRITICAL SUCCESS FACTORS	X
0.8 DEVELOPING YOUR OWN GUIDELINES	XI
1 SCOPE	1
2 TERMS AND DEFINITIONS	1
3 STRUCTURE OF THIS STANDARD	4
3.1 CLAUSES	4
3.2 MAIN SECURITY CATEGORIES	4
4 RISK ASSESSMENT AND TREATMENT	5
4.1 ASSESSING SECURITY RISKS	5
4.2 TREATING SECURITY RISKS.....	5
5 SECURITY POLICY	7
5.1 INFORMATION SECURITY POLICY	7
5.1.1 <i>Information security policy document</i>	7
5.1.2 <i>Review of the information security policy</i>	8
6 ORGANIZATION OF INFORMATION SECURITY	9
6.1 INTERNAL ORGANIZATION	9
6.1.1 <i>Management commitment to information security</i>	9
6.1.2 <i>Information security co-ordination</i>	10
6.1.3 <i>Allocation of information security responsibilities</i>	10
6.1.4 <i>Authorization process for information processing facilities</i>	11
6.1.5 <i>Confidentiality agreements</i>	11
6.1.6 <i>Contact with authorities</i>	12
6.1.7 <i>Contact with special interest groups</i>	12
6.1.8 <i>Independent review of information security</i>	13
6.2 EXTERNAL PARTIES	14
6.2.1 <i>Identification of risks related to external parties</i>	14
6.2.2 <i>Addressing security when dealing with customers</i>	15
6.2.3 <i>Addressing security in third party agreements</i>	16
7 ASSET MANAGEMENT	19
7.1 RESPONSIBILITY FOR ASSETS.....	19
7.1.1 <i>Inventory of assets</i>	19
7.1.2 <i>Ownership of assets</i>	20
7.1.3 <i>Acceptable use of assets</i>	20
7.2 INFORMATION CLASSIFICATION	21
7.2.1 <i>Classification guidelines</i>	21
7.2.2 <i>Information labeling and handling</i>	21
8 HUMAN RESOURCES SECURITY	23
8.1 PRIOR TO EMPLOYMENT	23
8.1.1 <i>Roles and responsibilities</i>	23

8.1.2	Screening	23
8.1.3	Terms and conditions of employment	24
8.2	DURING EMPLOYMENT	25
8.2.1	Management responsibilities	25
8.2.2	Information security awareness, education, and training	26
8.2.3	Disciplinary process	26
8.3	TERMINATION OR CHANGE OF EMPLOYMENT	27
8.3.1	Termination responsibilities	27
8.3.2	Return of assets	27
8.3.3	Removal of access rights	28
9	PHYSICAL AND ENVIRONMENTAL SECURITY	29
9.1	SECURE AREAS	29
9.1.1	Physical security perimeter	29
9.1.2	Physical entry controls	30
9.1.3	Securing offices, rooms, and facilities	30
9.1.4	Protecting against external and environmental threats	31
9.1.5	Working in secure areas	31
9.1.6	Public access, delivery, and loading areas	32
9.2	EQUIPMENT SECURITY	32
9.2.1	Equipment siting and protection	32
9.2.2	Supporting utilities	33
9.2.3	Cabling security	34
9.2.4	Equipment maintenance	34
9.2.5	Security of equipment off-premises	35
9.2.6	Secure disposal or re-use of equipment	35
9.2.7	Removal of property	36
10	COMMUNICATIONS AND OPERATIONS MANAGEMENT	37
10.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES	37
10.1.1	Documented operating procedures	37
10.1.2	Change management	37
10.1.3	Segregation of duties	38
10.1.4	Separation of development, test, and operational facilities	38
10.2	THIRD PARTY SERVICE DELIVERY MANAGEMENT	39
10.2.1	Service delivery	39
10.2.2	Monitoring and review of third party services	40
10.2.3	Managing changes to third party services	40
10.3	SYSTEM PLANNING AND ACCEPTANCE	41
10.3.1	Capacity management	41
10.3.2	System acceptance	41
10.4	PROTECTION AGAINST MALICIOUS AND MOBILE CODE	42
10.4.1	Controls against malicious code	42
10.4.2	Controls against mobile code	43
10.5	BACK-UP	44
10.5.1	Information back-up	44
10.6	NETWORK SECURITY MANAGEMENT	45
10.6.1	Network controls	45
10.6.2	Security of network services	46
10.7	MEDIA HANDLING	46
10.7.1	Management of removable media	46
10.7.2	Disposal of media	47
10.7.3	Information handling procedures	47
10.7.4	Security of system documentation	48
10.8	EXCHANGE OF INFORMATION	48
10.8.1	Information exchange policies and procedures	49
10.8.2	Exchange agreements	50
10.8.3	Physical media in transit	51
10.8.4	Electronic messaging	52
10.8.5	Business information systems	52

10.9	ELECTRONIC COMMERCE SERVICES	53
10.9.1	<i>Electronic commerce</i>	53
10.9.2	<i>On-Line Transactions</i>	54
10.9.3	<i>Publicly available information</i>	55
10.10	MONITORING	55
10.10.1	<i>Audit logging</i>	55
10.10.2	<i>Monitoring system use</i>	56
10.10.3	<i>Protection of log information</i>	57
10.10.4	<i>Administrator and operator logs</i>	58
10.10.5	<i>Fault logging</i>	58
10.10.6	<i>Clock synchronization</i>	58
11	ACCESS CONTROL	60
11.1	BUSINESS REQUIREMENT FOR ACCESS CONTROL	60
11.1.1	<i>Access control policy</i>	60
11.2	USER ACCESS MANAGEMENT	61
11.2.1	<i>User registration</i>	61
11.2.2	<i>Privilege management</i>	62
11.2.3	<i>User password management</i>	62
11.2.4	<i>Review of user access rights</i>	63
11.3	USER RESPONSIBILITIES	63
11.3.1	<i>Password use</i>	64
11.3.2	<i>Unattended user equipment</i>	64
11.3.3	<i>Clear desk and clear screen policy</i>	65
11.4	NETWORK ACCESS CONTROL	65
11.4.1	<i>Policy on use of network services</i>	66
11.4.2	<i>User authentication for external connections</i>	66
11.4.3	<i>Equipment identification in networks</i>	67
11.4.4	<i>Remote diagnostic and configuration port protection</i>	67
11.4.5	<i>Segregation in networks</i>	68
11.4.6	<i>Network connection control</i>	68
11.4.7	<i>Network routing control</i>	69
11.5	OPERATING SYSTEM ACCESS CONTROL	69
11.5.1	<i>Secure log-on procedures</i>	69
11.5.2	<i>User identification and authentication</i>	70
11.5.3	<i>Password management system</i>	71
11.5.4	<i>Use of system utilities</i>	72
11.5.5	<i>Session time-out</i>	72
11.5.6	<i>Limitation of connection time</i>	72
11.6	APPLICATION AND INFORMATION ACCESS CONTROL	73
11.6.1	<i>Information access restriction</i>	73
11.6.2	<i>Sensitive system isolation</i>	74
11.7	MOBILE COMPUTING AND TELEWORKING	74
11.7.1	<i>Mobile computing and communications</i>	74
11.7.2	<i>Teleworking</i>	75
12	INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	77
12.1	SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	77
12.1.1	<i>Security requirements analysis and specification</i>	77
12.2	CORRECT PROCESSING IN APPLICATIONS	78
12.2.1	<i>Input data validation</i>	78
12.2.2	<i>Control of internal processing</i>	78
12.2.3	<i>Message integrity</i>	79
12.2.4	<i>Output data validation</i>	79
12.3	CRYPTOGRAPHIC CONTROLS	80
12.3.1	<i>Policy on the use of cryptographic controls</i>	80
12.3.2	<i>Key management</i>	81
12.4	SECURITY OF SYSTEM FILES	83
12.4.1	<i>Control of operational software</i>	83
12.4.2	<i>Protection of system test data</i>	84

12.4.3	<i>Access control to program source code</i>	84
12.5	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	85
12.5.1	<i>Change control procedures</i>	85
12.5.2	<i>Technical review of applications after operating system changes</i>	86
12.5.3	<i>Restrictions on changes to software packages</i>	86
12.5.4	<i>Information leakage</i>	87
12.5.5	<i>Outsourced software development</i>	87
12.6	TECHNICAL VULNERABILITY MANAGEMENT	88
12.6.1	<i>Control of technical vulnerabilities</i>	88
13	INFORMATION SECURITY INCIDENT MANAGEMENT	90
13.1	REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES	90
13.1.1	<i>Reporting information security events</i>	90
13.1.2	<i>Reporting security weaknesses</i>	91
13.2	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	91
13.2.1	<i>Responsibilities and procedures</i>	92
13.2.2	<i>Learning from information security incidents</i>	93
13.2.3	<i>Collection of evidence</i>	93
14	BUSINESS CONTINUITY MANAGEMENT	95
14.1	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	95
14.1.1	<i>Including information security in the business continuity management process</i>	95
14.1.2	<i>Business continuity and risk assessment</i>	96
14.1.3	<i>Developing and implementing continuity plans including information security</i>	96
14.1.4	<i>Business continuity planning framework</i>	97
14.1.5	<i>Testing, maintaining and re-assessing business continuity plans</i>	98
15	COMPLIANCE.....	100
15.1	COMPLIANCE WITH LEGAL REQUIREMENTS	100
15.1.1	<i>Identification of applicable legislation</i>	100
15.1.2	<i>Intellectual property rights (IPR)</i>	100
15.1.3	<i>Protection of organizational records</i>	101
15.1.4	<i>Data protection and privacy of personal information</i>	102
15.1.5	<i>Prevention of misuse of information processing facilities</i>	102
15.1.6	<i>Regulation of cryptographic controls</i>	103
15.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	103
15.2.1	<i>Compliance with security policies and standards</i>	104
15.2.2	<i>Technical compliance checking</i>	104
15.3	INFORMATION SYSTEMS AUDIT CONSIDERATIONS	105
15.3.1	<i>Information systems audit controls</i>	105
15.3.2	<i>Protection of information systems audit tools</i>	105
BIBLIOGRAPHY.....		107
INDEX.....		108

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17799 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 17799:2000), which has been technically revised.

A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC JTC 1/SC 27. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into this new numbering scheme as ISO/IEC 27002.

0 Introduction

0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

0.3 How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements.

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.
2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.

0.4 Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More information about the assessment of security risks can be found in clause 4.1 "Assessing security risks".

0.5 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading "Information security starting point".

More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

0.6 Information security starting point

A number of controls can be considered as a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common practice for information security.

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

- a) data protection and privacy of personal information (see 15.1.4);
- b) protection of organizational records (see 15.1.3);
- c) intellectual property rights (see 15.1.2).

Controls considered to be common practice for information security include:

- a) information security policy document (see 5.1.1);
- b) allocation of information security responsibilities (see 6.1.3);
- c) information security awareness, education, and training (see 8.2.2);
- d) correct processing in applications (see 12.2);
- e) technical vulnerability management (see 12.6);
- f) business continuity management (see 14);
- g) management of information security incidents and improvements (see 13.2).

These controls apply to most organizations and in most environments.

It should be noted that although all controls in this standard are important and should be considered, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

0.7 Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- a) information security policy, objectives, and activities that reflect business objectives;
- b) an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
- c) visible support and commitment from all levels of management;
- d) a good understanding of the information security requirements, risk assessment, and risk management;
- e) effective marketing of information security to all managers, employees, and other parties to achieve awareness;
- f) distribution of guidance on information security policy and standards to all managers, employees and other parties;
- g) provision to fund information security management activities;
- h) providing appropriate awareness, training, and education;
- i) establishing an effective information security incident management process;
- j) implementation of a measurement¹ system that is used to evaluate performance in information security management and feedback suggestions for improvement.

¹ Note that information security measurements are outside of the scope of this standard.



The remainder of this document
is available for purchase online at

➤ www.saiglobal.com/shop ◀

SAI Global also carries a wide range of publications from a wide variety of Standards Publishers:



Click on the logos to search the database online.