



# SLOVENSKI STANDARD SIST ISO/IEC 27002:2008

01-maj-2008

---

Information technology - Security techniques - Code of practice for information security management / Note: Combines ISO/IEC 17799 (2005-06) (renumbered to ISO/IEC 27002) and ISO/IEC 17799 Technical Corrigendum 1 (2007-07)

**ITeH STANDARD PREVIEW**  
**(standards.iteh.ai)**

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

**Ta slovenski standard je istoveten z:**

---

**ICS:**

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding
--------	---------------------------------------	---------------------------------------

**SIST ISO/IEC 27002:2008**

**en**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST ISO/IEC 27002:2008

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

---

---

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

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

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27002:2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

[https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-  
b70bb8afbc37/sist-iso-iec-27002-2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

**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.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27002:2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>



**COPYRIGHT PROTECTED DOCUMENT**

© 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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

## 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 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27002 comprises ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007. Its technical content is identical to that of ISO/IEC 17799:2005. ISO/IEC 17799:2005/Cor.1:2007 changes the reference number of the standard from 17799 to 27002. ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007 are provisionally retained until publication of the second edition of ISO/IEC 27002.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST ISO/IEC 27002:2008

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>



**INTERNATIONAL STANDARD ISO/IEC 17799:2005  
TECHNICAL CORRIGENDUM 1**

Published 2007-07-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION  
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

## TECHNICAL CORRIGENDUM 1

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

RECTIFICATIF TECHNIQUE 1

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

Technical Corrigendum 1 to ISO/IEC 17799:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

<https://standards.iteh.ai/catalog/standards/sist/1980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

---

*Throughout the document:*

Replace “17799” with “27002”.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST ISO/IEC 27002:2008

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>



---

---

**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*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27002:2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

[https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-  
b70bb8afbc37/sist-iso-iec-27002-2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

**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.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27002:2008](https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008)

<https://standards.iteh.ai/catalog/standards/sist/f980af29-d798-4203-a199-b70bb8afbc37/sist-iso-iec-27002-2008>

© 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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

<b>Contents</b>	<b>Page</b>
<b>FOREWORD</b> .....	<b>VII</b>
<b>0 INTRODUCTION</b> .....	<b>VIII</b>
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
<b>1 SCOPE</b> .....	<b>1</b>
<b>2 TERMS AND DEFINITIONS</b> .....	<b>1</b>
<b>3 STRUCTURE OF THIS STANDARD</b> .....	<b>4</b>
3.1 CLAUSES .....	4
3.2 MAIN SECURITY CATEGORIES .....	4
<b>4 RISK ASSESSMENT AND TREATMENT</b> .....	<b>5</b>
4.1 ASSESSING SECURITY RISKS .....	5
4.2 TREATING SECURITY RISKS.....	5
<b>5 SECURITY POLICY</b> .....	<b>7</b>
5.1 INFORMATION SECURITY POLICY <small>ISO/IEC 27002:2008</small> .....	7
5.1.1 <i>Information security policy document</i> <small>ISO/IEC 27002:2008-1</small> .....	7
5.1.2 <i>Review of the information security policy</i> <small>ISO/IEC 27002:2008</small> .....	8
<b>6 ORGANIZATION OF INFORMATION SECURITY</b> .....	<b>9</b>
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
<b>7 ASSET MANAGEMENT</b> .....	<b>19</b>
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
<b>8 HUMAN RESOURCES SECURITY</b> .....	<b>23</b>
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
<b>9</b>	<b>PHYSICAL AND ENVIRONMENTAL SECURITY .....</b>	<b>29</b>
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
<b>10</b>	<b>COMMUNICATIONS AND OPERATIONS MANAGEMENT .....</b>	<b>37</b>
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

STANDARD PREVIEW  
(standards.iteh.ai)

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
<b>11</b>	<b>ACCESS CONTROL .....</b>	<b>60</b>
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
<b>12</b>	<b>INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE .....</b>	<b>77</b>
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	Access control to program source code.....	84
12.5	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES .....	85
12.5.1	Change control procedures .....	85
12.5.2	Technical review of applications after operating system changes.....	86
12.5.3	Restrictions on changes to software packages.....	86
12.5.4	Information leakage.....	87
12.5.5	Outsourced software development.....	87
12.6	TECHNICAL VULNERABILITY MANAGEMENT .....	88
12.6.1	Control of technical vulnerabilities .....	88
<b>13</b>	<b>INFORMATION SECURITY INCIDENT MANAGEMENT .....</b>	<b>90</b>
13.1	REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES .....	90
13.1.1	Reporting information security events.....	90
13.1.2	Reporting security weaknesses .....	91
13.2	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS .....	91
13.2.1	Responsibilities and procedures .....	92
13.2.2	Learning from information security incidents .....	93
13.2.3	Collection of evidence.....	93
<b>14</b>	<b>BUSINESS CONTINUITY MANAGEMENT .....</b>	<b>95</b>
14.1	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT .....	95
14.1.1	Including information security in the business continuity management process.....	95
14.1.2	Business continuity and risk assessment.....	96
14.1.3	Developing and implementing continuity plans including information security .....	96
14.1.4	Business continuity planning framework.....	97
14.1.5	Testing, maintaining and re-assessing business continuity plans.....	98
<b>15</b>	<b>COMPLIANCE..... (standards.iteh.ai)</b>	<b>100</b>
15.1	COMPLIANCE WITH LEGAL REQUIREMENTS .....	100
15.1.1	Identification of applicable legislation <a href="http://standards.iso.org/standards/catalog/standards/sist/980af29-d798-4203-a199-770002008">ISO/IEC 27002:2008</a> .....	100
15.1.2	Intellectual property rights (IPR) <a href="http://standards.iso.org/standards/catalog/standards/sist/980af29-d798-4203-a199-770002008">catalog/standards/sist/980af29-d798-4203-a199-770002008</a> .....	100
15.1.3	Protection of organizational records <a href="http://standards.iso.org/standards/catalog/standards/sist/980af29-d798-4203-a199-770002008">catalog/standards/sist/980af29-d798-4203-a199-770002008</a> .....	101
15.1.4	Data protection and privacy of personal information .....	102
15.1.5	Prevention of misuse of information processing facilities .....	102
15.1.6	Regulation of cryptographic controls.....	103
15.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE .....	103
15.2.1	Compliance with security policies and standards.....	104
15.2.2	Technical compliance checking.....	104
15.3	INFORMATION SYSTEMS AUDIT CONSIDERATIONS .....	105
15.3.1	Information systems audit controls.....	105
15.3.2	Protection of information systems audit tools .....	105
<b>BIBLIOGRAPHY.....</b>		<b>107</b>
<b>INDEX.....</b>		<b>108</b>

## 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.