



SLOVENSKI STANDARD
oSIST ISO/IEC FDIS 27002:2013
01-september-2013

Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri nadzoru informacijske varnosti

Information technology -- Security techniques -- Code of practice for information security controls

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

Ta slovenski standard je istoveten z: ISO/IEC FDIS 27002

ICS:

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

oSIST ISO/IEC FDIS 27002:2013 **en,fr,de**

FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
27002

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2013-07-03

Voting terminates on:
2013-09-03

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number
ISO/IEC FDIS 27002:2013(E)

© ISO/IEC 2013

ISO/IEC FDIS 27002:2013(E)

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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	v
0 Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this standard	1
4.1 Clauses	1
4.2 Control categories	1
5 Information security policies	2
5.1 Management direction for information security	2
6 Organization of information security	4
6.1 Internal organization	4
6.2 Mobile devices and teleworking	6
7 Human resource security	9
7.1 Prior to employment	9
7.2 During employment	10
7.3 Termination and change of employment	13
8 Asset management	13
8.1 Responsibility for assets	13
8.2 Information classification	15
8.3 Media handling	17
9 Access control	19
9.1 Business requirements of access control	19
9.2 User access management	21
9.3 User responsibilities	24
9.4 System and application access control	25
10 Cryptography	28
10.1 Cryptographic controls	28
11 Physical and environmental security	30
11.1 Secure areas	30
11.2 Equipment	33
12 Operations security	38
12.1 Operational procedures and responsibilities	38
12.2 Protection from malware	41
12.3 Backup	42
12.4 Logging and monitoring	43
12.5 Control of operational software	45
12.6 Technical vulnerability management	46
12.7 Information systems audit considerations	48
13 Communications security	49
13.1 Network security management	49
13.2 Information transfer	50
14 System acquisition, development and maintenance	54
14.1 Security requirements of information systems	54
14.2 Security in development and support processes	57
14.3 Test data	62
15 Supplier relationships	62
15.1 Information security in supplier relationships	62

ISO/IEC FDIS 27002:2013(E)

15.2	Supplier service delivery management	66
16	Information security incident management	67
16.1	Management of information security incidents and improvements	67
17	Information security aspects of business continuity management	71
17.1	Information security continuity	71
17.2	Redundancies	73
18	Compliance	74
18.1	Compliance with legal and contractual requirements	74
18.2	Information security reviews	77
Bibliography		80

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.

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

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

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised.

ISO/IEC FDIS 27002:2013(E)

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

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. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. 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. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

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

- a) 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;
- b) legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;