

---

---

**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*

Sýnishorn

Sýnishorn



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

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>0 Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Structure of this standard</b> .....	<b>1</b>
4.1 Clauses.....	1
4.2 Control categories.....	1
<b>5 Information security policies</b> .....	<b>2</b>
5.1 Management direction for information security.....	2
<b>6 Organization of information security</b> .....	<b>4</b>
6.1 Internal organization.....	4
6.2 Mobile devices and teleworking.....	6
<b>7 Human resource security</b> .....	<b>9</b>
7.1 Prior to employment.....	9
7.2 During employment.....	10
7.3 Termination and change of employment.....	13
<b>8 Asset management</b> .....	<b>13</b>
8.1 Responsibility for assets.....	13
8.2 Information classification.....	15
8.3 Media handling.....	17
<b>9 Access control</b> .....	<b>19</b>
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
<b>10 Cryptography</b> .....	<b>28</b>
10.1 Cryptographic controls.....	28
<b>11 Physical and environmental security</b> .....	<b>30</b>
11.1 Secure areas.....	30
11.2 Equipment.....	33
<b>12 Operations security</b> .....	<b>38</b>
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
<b>13 Communications security</b> .....	<b>49</b>
13.1 Network security management.....	49
13.2 Information transfer.....	50
<b>14 System acquisition, development and maintenance</b> .....	<b>54</b>
14.1 Security requirements of information systems.....	54
14.2 Security in development and support processes.....	57
14.3 Test data.....	62
<b>15 Supplier relationships</b> .....	<b>62</b>
15.1 Information security in supplier relationships.....	62

15.2	Supplier service delivery management.....	66
<b>16</b>	<b>Information security incident management.....</b>	<b>67</b>
16.1	Management of information security incidents and improvements.....	67
<b>17</b>	<b>Information security aspects of business continuity management.....</b>	<b>71</b>
17.1	Information security continuity.....	71
17.2	Redundancies.....	73
<b>18</b>	<b>Compliance.....</b>	<b>74</b>
18.1	Compliance with legal and contractual requirements.....	74
18.2	Information security reviews.....	77
	<b>Bibliography.....</b>	<b>79</b>

Sýnishorn

## 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.

Sýnishorn