

INTERNATIONAL
STANDARD

ISO/IEC
27002

Second edition
2013-10-01

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

ISO/IEC 27002:2013 - Preview only Copy via ILNAS e-Shop

Reference number
ISO/IEC 27002:2013(E)



© ISO/IEC 2013



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