

ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 27002:2017

**Information technology - Security
techniques - Code of practice for
information security controls (ISO/IEC
27002:2013 including Cor 1:2014 and**

Informationstechnik -
Sicherheitsverfahren - Leitfaden für
Informationssicherheitsmaßnahmen
(ISO/IEC 27002:2013 einschließlich Cor

Technologies de l'information -
Techniques de sécurité - Code de bonne
pratique pour le management de la
sécurité de l'information (ISO/IEC

02/2017



National Foreword

This European Standard EN ISO/IEC 27002:2017 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 27002:2017.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

THIS PUBLICATION IS COPYRIGHT PROTECTED

Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!

ILNAS-EN ISO/IEC 27002:2017

EUROPEAN STANDARD **EN ISO/IEC 27002**

NORME EUROPÉENNE

EUROPÄISCHE NORM

February 2017

ICS 03.100.70; 35.030

English Version

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité
- Code de bonne pratique pour le management de la
sécurité de l'information (ISO/IEC 27002:2013 y
compris Cor 1:2014 et Cor 2:2015)

Informationstechnik - Sicherheitsverfahren - Leitfaden
für Informationssicherheitsmaßnahmen (ISO/IEC
27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

This European Standard was approved by CEN on 26 January 2017.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword..... 3

European foreword

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27002:2017.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by August 2017, and conflicting national standards shall be withdrawn at the latest by August 2017.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015 has been approved by CEN as EN ISO/IEC 27002:2017 without any modification.

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*





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

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.....	79