ILNAS

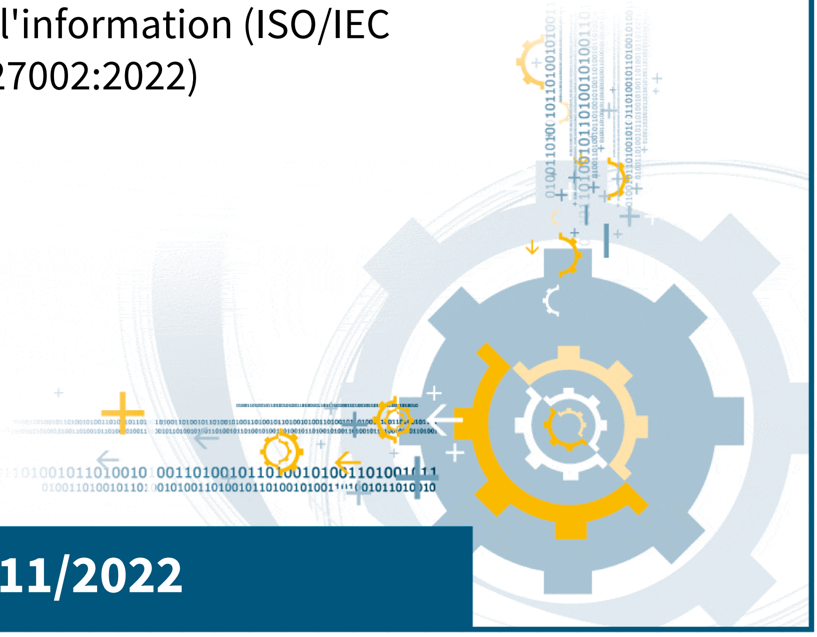
Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information (ISO/IEC 27002:2022)



11/2022

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

National Foreword

This European Standard EN ISO/IEC 27002:2022 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 27002:2022.

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

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

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!

EUROPEAN STANDARD **EN ISO/IEC 27002**

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2022

ICS 35.030

Supersedes EN ISO/IEC 27002:2017

English version

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Moyens de maîtrise de l'information (ISO/IEC 27002:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

This European Standard was approved by CEN on 30 October 2022.

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 and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2022 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

ILNAS-EN ISO/IEC 27002:2022

Contents

Page

European foreword 3

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

European foreword

The text of ISO/IEC 27002:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology” of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27002:2022 by Technical Committee CEN-CENELEC/ JTC 13 “Cybersecurity and Data Protection” the secretariat of which is held by DIN.

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 May 2023, and conflicting national standards shall be withdrawn at the latest by May 2023.

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

This document supersedes EN ISO/IEC 27002:2017.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27002:2022 has been approved by CEN-CENELEC as EN ISO/IEC 27002:2022 without any modification.

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Reference number
ISO/IEC 27002:2022(E)

© ISO/IEC 2022

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

Contents

Page

Foreword .... **vi**

Introduction .... **vii**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 6

4 Structure of this document **7**
4.1 Clauses 7
4.2 Themes and attributes 8
4.3 Control layout 9

5 Organizational controls **9**
5.1 Policies for information security 9
5.2 Information security roles and responsibilities 11
5.3 Segregation of duties 12
5.4 Management responsibilities 13
5.5 Contact with authorities 14
5.6 Contact with special interest groups 15
5.7 Threat intelligence 15
5.8 Information security in project management 17
5.9 Inventory of information and other associated assets 18
5.10 Acceptable use of information and other associated assets 20
5.11 Return of assets 21
5.12 Classification of information 22
5.13 Labelling of information 23
5.14 Information transfer 24
5.15 Access control 27
5.16 Identity management 29
5.17 Authentication information 30
5.18 Access rights 32
5.19 Information security in supplier relationships 33
5.20 Addressing information security within supplier agreements 35
5.21 Managing information security in the ICT supply chain 37
5.22 Monitoring, review and change management of supplier services 39
5.23 Information security for use of cloud services 41
5.24 Information security incident management planning and preparation 43
5.25 Assessment and decision on information security events 44
5.26 Response to information security incidents 45
5.27 Learning from information security incidents 46
5.28 Collection of evidence 46
5.29 Information security during disruption 48
5.30 ICT readiness for business continuity 48
5.31 Legal, statutory, regulatory and contractual requirements 50
5.32 Intellectual property rights 51
5.33 Protection of records 53
5.34 Privacy and protection of PII 54
5.35 Independent review of information security 55
5.36 Compliance with policies, rules and standards for information security 56
5.37 Documented operating procedures 57

6 People controls **58**
6.1 Screening 58
6.2 Terms and conditions of employment 59

6.3 Information security awareness, education and training 60
6.4 Disciplinary process 62
6.5 Responsibilities after termination or change of employment 63
6.6 Confidentiality or non-disclosure agreements 63
6.7 Remote working 65
6.8 Information security event reporting 66

7 Physical controls 67
7.1 Physical security perimeters 67
7.2 Physical entry 68
7.3 Securing offices, rooms and facilities 70
7.4 Physical security monitoring 70
7.5 Protecting against physical and environmental threats 71
7.6 Working in secure areas 72
7.7 Clear desk and clear screen 73
7.8 Equipment siting and protection 74
7.9 Security of assets off-premises 75
7.10 Storage media 76
7.11 Supporting utilities 77
7.12 Cabling security 78
7.13 Equipment maintenance 79
7.14 Secure disposal or re-use of equipment 80

8 Technological controls 81
8.1 User endpoint devices 81
8.2 Privileged access rights 83
8.3 Information access restriction 84
8.4 Access to source code 86
8.5 Secure authentication 87
8.6 Capacity management 89
8.7 Protection against malware 90
8.8 Management of technical vulnerabilities 92
8.9 Configuration management 95
8.10 Information deletion 97
8.11 Data masking 98
8.12 Data leakage prevention 100
8.13 Information backup 101
8.14 Redundancy of information processing facilities 102
8.15 Logging 103
8.16 Monitoring activities 106
8.17 Clock synchronization 108
8.18 Use of privileged utility programs 109
8.19 Installation of software on operational systems 110
8.20 Networks security 111
8.21 Security of network services 112
8.22 Segregation of networks 113
8.23 Web filtering 114
8.24 Use of cryptography 115
8.25 Secure development life cycle 117
8.26 Application security requirements 118
8.27 Secure system architecture and engineering principles 120
8.28 Secure coding 122
8.29 Security testing in development and acceptance 124
8.30 Outsourced development 126
8.31 Separation of development, test and production environments 127
8.32 Change management 128
8.33 Test information 129
8.34 Protection of information systems during audit testing 130

Annex A (informative) **Using attributes 132**

ILNAS-EN ISO/IEC 27002:2022 - Preview only Copy via ILNAS e-Shop

© ISO/IEC 2022 – All rights reserved