

ILNAS

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

ILNAS-EN 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)

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

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

11/2022



Avant-propos national

Cette Norme Européenne EN ISO/IEC 27002:2022 a été adoptée comme Norme Luxembourgeoise ILNAS-EN ISO/IEC 27002:2022.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

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

CETTE PUBLICATION EST PROTÉGÉE PAR LE DROIT D'AUTEUR

Aucun contenu de la présente publication ne peut être reproduit ou utilisé sous quelque forme ou par quelque procédé que ce soit - électronique, mécanique, photocopie ou par d'autres moyens sans autorisation préalable !

ILNAS-EN ISO/IEC 27002:2022
NORME EUROPÉENNE **EN ISO/IEC 27002**
EUROPÄISCHE NORM
EUROPEAN STANDARD

Novembre 2022

ICS 35.030

Remplace l' EN ISO/IEC 27002:2017

Version Française

**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)

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

La présente Norme européenne a été adoptée par le CEN le 30 octobre 2022.

Les membres du CEN et CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN et CENELEC.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN et CENELEC dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN et du CENELEC sont les organismes nationaux de normalisation et les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.



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

Sommaire

Page

Avant-propos européen 3

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

Avant-propos européen

Le texte de l'ISO/IEC 27002:2022 a été élaboré par le Comité technique ISO/IEC JTC 1 « Technologies de l'information » de l'Organisation internationale de normalisation (ISO) et a été repris comme EN ISO/IEC 27002:2022 par le Comité technique CEN-CENELEC/ JTC 13 « Cybersécurité et protection des données » dont le secrétariat est tenu par DIN.

La présente Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en mai 2023 et les normes nationales en contradiction devront être retirées au plus tard en mai 2023.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CEN et/ou le CENELEC ne sauraient être tenus pour responsables de l'identification de ces droits de propriété en tout ou partie.

Ce document remplace l'EN ISO/IEC 27002:2017.

Il convient que l'utilisateur adresse tout retour d'information et toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve sur les sites web du CEN et du CENELEC.

Selon le règlement intérieur du CEN/CENELEC, les instituts de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Notice d'entérinement

Le texte de l'ISO/IEC 27002:2022 a été approuvé par le CEN-CENELEC comme EN ISO/IEC 27002:2022 sans aucune modification.

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

*Information security, cybersecurity and privacy protection —
Information security controls*

**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO/IEC 2022

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office

Case postale 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Genève

Tél.: +41 22 749 01 11

Fax: +41 22 749 09 47

E-mail: copyright@iso.org

Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	vi
Introduction	vii
1 Domaine d'application	1
2 Références normatives	1
3 Termes, définitions et abréviations	1
3.1 Termes et définitions	1
3.2 Abréviations	6
4 Structure du présent document	8
4.1 Articles	8
4.2 Thèmes et attributs	8
4.3 Structure des mesures de sécurité	9
5 Mesures de sécurité organisationnelles	10
5.1 Politiques de sécurité de l'information	10
5.2 Fonctions et responsabilités liées à la sécurité de l'information	12
5.3 Séparation des tâches	13
5.4 Responsabilités de la direction	14
5.5 Contacts avec les autorités	15
5.6 Contacts avec des groupes d'intérêt spécifiques	16
5.7 Renseignements sur les menaces	17
5.8 Sécurité de l'information dans la gestion de projet	18
5.9 Inventaire des informations et autres actifs associés	20
5.10 Utilisation correcte des informations et autres actifs associés	22
5.11 Restitution des actifs	23
5.12 Classification des informations	24
5.13 Marquage des informations	25
5.14 Transfert des informations	27
5.15 Contrôle d'accès	29
5.16 Gestion des identités	31
5.17 Informations d'authentification	33
5.18 Droits d'accès	35
5.19 Sécurité de l'information dans les relations avec les fournisseurs	36
5.20 La sécurité de l'information dans les accords conclus avec les fournisseurs	39
5.21 Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC	41
5.22 Surveillance, révision et gestion des changements des services fournisseurs	43
5.23 Sécurité de l'information dans l'utilisation de services en nuage	44
5.24 Planification et préparation de la gestion des incidents de sécurité de l'information	47
5.25 Évaluation des événements de sécurité de l'information et prise de décision	49
5.26 Réponse aux incidents de sécurité de l'information	49
5.27 Tirer des enseignements des incidents de sécurité de l'information	50
5.28 Collecte des preuves	51
5.29 Sécurité de l'information pendant une perturbation	52
5.30 Préparation des TIC pour la continuité d'activité	53
5.31 Exigences légales, statutaires, réglementaires et contractuelles	54
5.32 Droits de propriété intellectuelle	56
5.33 Protection des enregistrements	57
5.34 Protection de la vie privée et des DCP	59
5.35 Révision indépendante de la sécurité de l'information	60
5.36 Conformité aux politiques, règles et normes de sécurité de l'information	61
5.37 Procédures d'exploitation documentées	62
6 Mesures de sécurité applicables aux personnes	63
6.1 Sélection des candidats	63
6.2 Termes et conditions du contrat de travail	64

6.3	Sensibilisation, enseignement et formation en sécurité de l'information.....	66
6.4	Processus disciplinaire.....	67
6.5	Responsabilités après la fin ou le changement d'un emploi.....	68
6.6	Accords de confidentialité ou de non-divulgateion.....	69
6.7	Travail à distance.....	70
6.8	Déclaration des événements de sécurité de l'information.....	72
7	Mesures de sécurité physique.....	73
7.1	Périmètres de sécurité physique.....	73
7.2	Les entrées physiques.....	74
7.3	Sécurisation des bureaux, des salles et des installations.....	76
7.4	Surveillance de la sécurité physique.....	77
7.5	Protection contre les menaces physiques et environnementales.....	78
7.6	Travail dans les zones sécurisées.....	79
7.7	Bureau vide et écran vide.....	80
7.8	Emplacement et protection du matériel.....	81
7.9	Sécurité des actifs hors des locaux.....	82
7.10	Supports de stockage.....	83
7.11	Services supports.....	85
7.12	Sécurité du câblage.....	86
7.13	Maintenance du matériel.....	87
7.14	Élimination ou recyclage sécurisé(e) du matériel.....	88
8	Mesures de sécurité technologiques.....	89
8.1	Terminaux finaux des utilisateurs.....	89
8.2	Droits d'accès privilégiés.....	91
8.3	Restrictions d'accès aux informations.....	93
8.4	Accès aux codes source.....	95
8.5	Authentification sécurisée.....	96
8.6	Dimensionnement.....	97
8.7	Protection contre les programmes malveillants (<i>malware</i>).....	99
8.8	Gestion des vulnérabilités techniques.....	101
8.9	Gestion des configurations.....	104
8.10	Suppression des informations.....	106
8.11	Masquage des données.....	108
8.12	Prévention de la fuite de données.....	110
8.13	Sauvegarde des informations.....	111
8.14	Redondance des moyens de traitement de l'information.....	113
8.15	Journalisation.....	114
8.16	Activités de surveillance.....	117
8.17	Synchronisation des horloges.....	119
8.18	Utilisation de programmes utilitaires à privilèges.....	120
8.19	Installation de logiciels sur des systèmes opérationnels.....	121
8.20	Sécurité des réseaux.....	122
8.21	Sécurité des services réseau.....	123
8.22	Cloisonnement des réseaux.....	125
8.23	Filtrage web.....	126
8.24	Utilisation de la cryptographie.....	127
8.25	Cycle de vie de développement sécurisé.....	129
8.26	Exigences de sécurité des applications.....	130
8.27	Principes d'ingénierie et d'architecture des systèmes sécurisés.....	132
8.28	Codage sécurisé.....	134
8.29	Tests de sécurité dans le développement et l'acceptation.....	137
8.30	Développement externalisé.....	138
8.31	Séparation des environnements de développement, de test et opérationnels.....	139
8.32	Gestion des changements.....	141
8.33	Informations de test.....	142
8.34	Protection des systèmes d'information pendant les tests d'audit.....	143
	Annexe A (informative) Utilisation des attributs.....	145