

ILNAS

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

ILNAS 107:2020

Sécurité de l'information dans le cadre de l'accréditation de laboratoires

Sommaire

	Page
Avant-propos.....	3
Introduction	4
1 Domaine d'application	5
2 Références normatives	5
3 Termes et définitions	6
4 Exigences de sécurité de l'information au laboratoire	8
5 Objectif et mesures de mise en œuvre de la sécurité de l'information au laboratoire	8
5.1 Objectif	8
5.2 Mesures	11
5.2.1 Disponibilité et intégrité de la documentation relative aux actifs de support	11
5.2.2 Rôles et responsabilités	12
5.2.3 Gestion des changements	13
5.2.4 Gestion des accès	15
5.2.5 Sauvegarde des actifs de support	16
5.2.6 Conditions environnementales	17
5.2.7 Stockage des actifs de support	18
5.2.8 Protection des données	18
5.2.9 Transfert de l'information	19
5.2.10 Continuité des activités	20
5.2.11 Conformité des fournisseurs	21
Annexe A (informative) Tableau récapitulatif des mesures de sécurité de l'information	22
Annexe B (informative) Tableau récapitulatif de l'ensemble des dispositions/bonnes pratiques relatives à la sécurité de l'information	23
Annexe C (informative) Exemples de risques génériques à considérer	24
Annexe D (informative) Exemples de questions d'audit	29
D.1 Questions relatives à l'objectif	29
D.2 Questions relatives aux mesures	30
D.2.1 Disponibilité et intégrité de la documentation relative aux actifs de support	30
D.2.2 Rôles et responsabilités	30
D.2.3 Gestion des changements	31
D.2.4 Gestion des accès	31
D.2.5 Sauvegarde des actifs de support	32
D.2.6 Conditions environnementales	32
D.2.7 Stockage des actifs de support	33
D.2.8 Protection des données	34
D.2.9 Transfert de l'information	34
D.2.10 Continuité des activités	35
D.2.11 Conformité des fournisseurs	36
Bibliographie	37

Avant-propos

La présente norme luxembourgeoise (ILNAS 107:2020) a été élaborée par le groupe de travail « Sécurité de l'information (SI) dans les laboratoires » mis en place sous la responsabilité et la présidence de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS).

La référence à cette norme luxembourgeoise devra être publiée au Journal officiel du Grand-Duché de Luxembourg pour recevoir le statut de norme nationale.

Une attention particulière est portée au fait que certains des éléments du présent document peuvent être soumis à des droits de propriété intellectuelle ou des droits analogues. L'ILNAS ne saurait être tenu pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

Le présent document a été élaboré dans le cadre de l'accréditation des laboratoires de biologie médicale selon la norme ILNAS-EN ISO 15189:2012 et des laboratoires d'étalonnages et d'essais selon la norme ILNAS-EN ISO/IEC 17025:2017.

Note : Dans le présent document, les textes marqués en « *italique* » sont des extraits des normes ILNAS-EN ISO 15189:2012 et ILNAS-EN ISO/IEC 17025:2017. La publication partielle de ces extraits a été approuvée par l'ILNAS en sa qualité d'Organisme luxembourgeois de normalisation (OLN) et membre du Comité européen de normalisation (CEN).

Introduction

En considérant l'importance accrue de la digitalisation et de l'évolution des services numériques de support de la gestion de la qualité et du traitement des processus métier dans les laboratoires, le présent document relatif aux exigences en matière de sécurité de l'information dans les laboratoires a pour objectifs :

- d'offrir une interprétation plus approfondie des exigences formulées dans les deux normes ILNAS-EN ISO 15189:2012 et ILNAS-EN ISO/IEC 17025:2017 ;
- de proposer des recommandations pour l'implémentation de mesures adéquates en matière de sécurité de l'information dans les laboratoires, adaptées à leurs besoins ;
- de se focaliser sur l'approche par les risques adoptée par les laboratoires en matière de sécurité de l'information ;
- de fournir davantage de recommandations aux auditeurs de l'Office Luxembourgeois d'Accréditation et de Surveillance (OLAS) pour auditer les aspects liés à la sécurité de l'information dans le cadre d'un audit d'accréditation.

Le présent document peut contribuer à aider les laboratoires à se conformer à l'article 32 « Sécurité du traitement » du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (RGPD) [1].

Le présent document peut servir de bonnes pratiques aux laboratoires du secteur public pour se conformer à la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte [2].