MYXLAB GIE - Biologie médicale

Politique de Sécurité des Systèmes d'Informations

_I1PRPSSI

Version : 01	**Date de validation :** 05/03/2024
Type de texte : Procédure	**Date de mis en application :** 05/03/2024

	Intervenants	Dates
Auteur	PEROL Eliane	15/12/2023
Vérification	COMY Eric	22/02/2024
Approbation	[redacted]	01/03/2024

Historique des versions

NOMVERSION	COMMENTAIRE	VALIDE	DATE
Politique de Sécurité des Systèmes d'Informations	01	Oui	05/03/2024

Référentiels

NORME	CHAPITRE	SOUSCHAPITRE	PARAGRAPHE
Norme NF EN ISO 15189 - dec 2022	7 - Exigences relatives aux processus	7.6 - Maîtrise des données et gestion de l'information	

Distribution

[redacted]

MYXLAB GIE - Biologie médicale

Politique de Sécurité des Systèmes d'Informations

_I1PRPSSI

Table des matières

Politique de Sécurité des Systèmes d'Informations

_I1PRPSSI

Politique de Sécurité des Systèmes d'Informations

_I1PRPSSI

Politique de sécurité des systèmes d'information

Les modifications par rapport à la version précédente apparaissent en rouge.

Préambule

Le système d'information remplit des fonctions indispensables à la prise en charge des examens biologiques comme à la gestion quotidienne du laboratoire.
Certaines informations traitées par le système d'information sont particulièrement sensibles, comme les données de santé des patients et leurs résultats d'analyse. Notre système d'information doit garantir que ces informations restent authentiques et confidentielles. Son ouverture vers l'extérieur avec nos partenaires (cliniques, laboratoires, établissements de soins, institutions, etc.) doit se faire dans un cadre sécurisé et maîtrisé.
Ces mêmes données sont exposées à des menaces et des risques réels, notamment de vol et de négligence, pouvant engager la responsabilité de tous.
Au regard de ces risques, le laboratoire a la responsabilité vis-à-vis des patients et de ses partenaires de garantir un niveau de sécurité suffisant pour protéger les données qui lui sont confiées.
Pour relever ce défi, une politique de sécurité a été élaborée pour mettre en œuvre un plan d'action sécurité visant à permettre de maîtriser les risques.
La présente politique de sécurité des systèmes d'information constitue le cadre unique de référence du laboratoire pour toutes les questions de sécurité des systèmes d'information.
Chacun doit veiller personnellement à sa bonne mise en application, et faire preuve de vigilance dans son usage des moyens de traitement des informations.

Le Directeur Général

Le Responsable des Systèmes d'Information

Politique de Sécurité des Systèmes d'Informations

_I1PRPSSI

1. Objet et domaine d'application

La Politique de Sécurité des Systèmes d'Information (PSSI) décline la stratégie de sécurité au travers de mesures relevant de la sécurité des systèmes d'information (SSI). Elle constitue le document maître du référentiel de SSI.

La PSSI vise à couvrir l'ensemble des risques pesant sur les informations et traitements des systèmes d'information du laboratoire.

Elle est structurée selon les chapitres de la norme ISO/CEI 27002:2013, document regroupant les bonnes pratiques en matière de gestion de la sécurité de l'information, selon divers axes exprimés dans les chapitres du présent document.

1.1 Périmètre d'applicabilité et exclusion

Ce document est amené à remplacer en totalité ou partiellement les procédures de Maîtrise de l'informatique I1PR01 et de la mâitrise du SIL I1PR02

La PSSI est applicable à l'ensemble des personnels présents dans l'Entreprise (salariés, stagiaires, intérimaires, prestataires de services), mais également à ceux ayant la possibilité d'accéder à distance directement aux systèmes d'information du laboratoire**.**

Il s'agit en premier lieu des collaborateurs salariés, mais également, sans que cette liste soit exhaustive :

- Des partenaires opérationnels (sous-traitants, cliniques, laboratoires, etc.),
- Des prestataires externes.

Elle est également applicable à toute ressource informatique, et ce quelle que soit leur origine (fournie par la DSI, achetée par une unité, etc.), appartenant aux systèmes d'information, par exemple, sans que cette liste soit exhaustive :

- Serveurs,
- Postes de travail,
- Terminaux mobiles,
- Périphériques de stockage amovibles, supports de stockage ou d'archivage,
- Photocopieurs, imprimantes, scanners,
- Équipements réseaux, de télécommunication,
- Logiciels,
- Automates.

La PSSI prend en compte les besoins de protection de l'Information, de protection du patrimoine scientifique et technique du laboratoire.

Il peut être nécessaire, dans certains cas, de déroger à des règles énoncées par la PSSI. Il appartient alors au Responsable informatique de leur substituer formellement des règles spécifiques. La décision de dérogation, accompagnée de la justification, est tenue à la disposition des autorités.

Les points ci-dessous ne sont pas traités dans ce document :

- La sécurité des biens et des personnes,
- La sécurité physique des bâtiments,
- Le traitement des risques hors périmètre de la sécurité des systèmes d'information

1.2 Mode de validation et révision du document

L'élaboration de cette procédure est soumise à un plan d'action SapaNet n°1496.
La PSSI pourra se substituer en totalité ou en partie aux procédures IPR01 Maîtrise du système informatique et I1PR02 Validation et maîtrise du SIL. Ces dernières seront révisées ou supprimées après validation de cette procédure.

La PSSI est validée par le comité de direction du laboratoire et de son responsable des systèmes d'information.

La PSSI est régulièrement révisée, au moins une fois tous les 2 ans. Ces révisions garantissent son adéquation avec les enjeux du laboratoire, son efficacité dans le temps et son applicabilité.

La PSSI est diffusée aux personnes concernées à partir de l'outil de gestion documentaire qualité.

1.3 Les enjeux majeurs de la sécurité des SI

La mission essentielle du laboratoire est de fournir des analyses biomédicales dont dépend la chaîne de soin, tout en respectant l'équité des soins.

Le laboratoire a pour priorité de respecter la confidentialité des données des patients et des collaborateurs, de rechercher toujours plus de qualité et enfin d'acquérir dès que possible plus de performance.

La bonne réalisation de sa mission dépend également du support interne (informatique, logistique, ressources humaines, hygiène et sécurité, secrétariat médical, approvisionnement, communication, marketing, qualité).

Cette mission essentielle s'appuie sur de l'information de sensibilité diverse, stockée sur différents systèmes d'information et constituant le patrimoine informationnel de l'entreprise.

Le laboratoire est confrontée à des menaces et des vulnérabilités sur ses systèmes d'information :

- Menaces externes : cybercriminels, concurrence, organisations activistes ou terroristes,
- Menaces et vulnérabilités internes : utilisateurs insuffisamment sensibilisés, utilisateurs malveillants, mauvaise qualité ou obsolescence de système, défaut de sécurité des automates

Les impacts possibles sont d'ordres différents. Les menaces affectant les informations ou les ressources peuvent entraîner des :

- Retards de livraison des résultats d'analyse ou perte de capacité à mener des analyses
- Pertes de confiance dans les résultats transmis
- Non-conformité réglementaire
- Perte de confidentialité des données médicales ou à caractère personnel
- Pertes financières
- Atteinte à l'image ou à la réputation Objectifs de sécurité

Afin de faire face à cet environnement à risque, le laboratoire se fixe différents objectifs :

• Mettre en place une gouvernance de la sécurité en attribuant les rôles sécurités et en maintenant les documentations à jour.

• Anticiper et préparer la réaction aux incidents de sécurité. Cf plan d'action n°1497

.• Concevoir, mettre en œuvre et opérer des systèmes d'information performant en garantissant une prise en compte efficace et effective de la sécurité des traitements et des informations collectées et traitée. Cela passe par la maîtrise des accès, le traitement des vulnérabilités, le cloisonnement des systèmes et le chiffrement des données.

• Respecter les différentes lois et réglementations et s'assurer de la mise en conformité de ses systèmes d'information à celles-ci.

2 . Organisation de la sécurité des systèmes d'information

2.1 Référentiel documentaire sécurité

La PSSI constitue le document fondateur de la prise en compte de la sécurité au sein du laboratoire.
Celle-ci est déclinée selon différents sujets ou publics afin de constituer un référentiel applicable à tous niveaux.
Le référentiel documentaire de la sécurité adopté s'inscrit dans le référentiel existant pour les laboratoires de biologie médicale.
Les documents liés à la sécurité sont régulièrement mis à jour et mis à disposition dans l'outil de gestion documentaire qualité.

2.2 Répartition des rôles sécurité

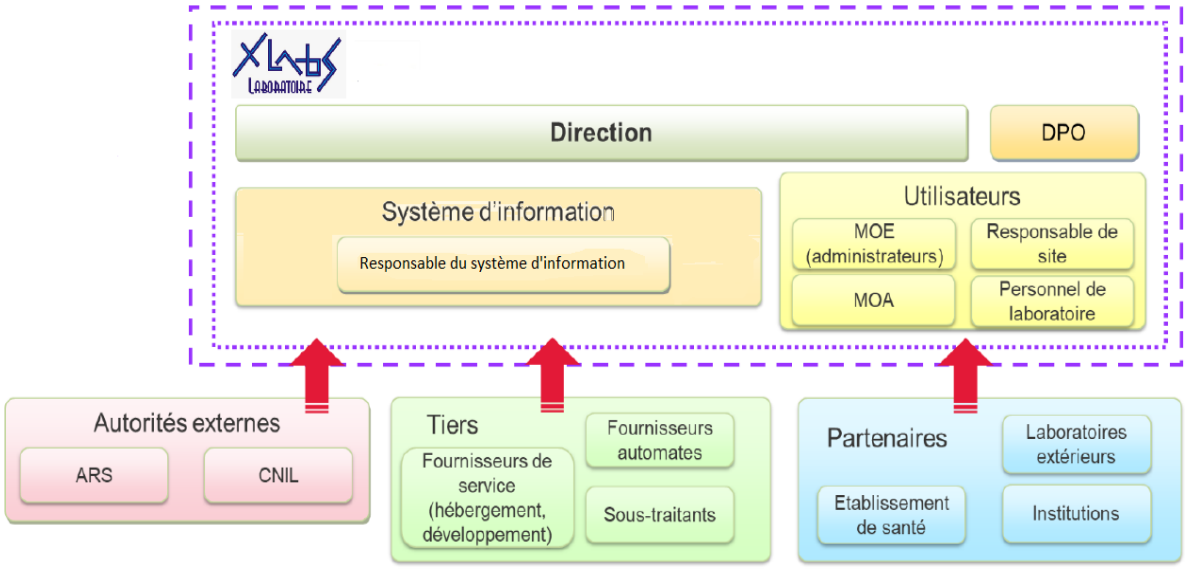

Figure : Organisation de la sécurité

MOA : définit et pilote le projet, MOE : exécute techniquement le projet