



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*

Inserm



La science pour la santé
From science to health



Politique Générale des Systèmes d'Information de l'INSERM

01/07/2026

Identification du document

Identification du document		
Document	Sujet	Version du document
PSSI	Politique de Sécurité des Systèmes d'Information	V1.2

Approbation du document			
Nom	Fonction	Date	Action
Vincent ARCHER	RSSI	01/07/2026	Rédaction
Zi-Long LI	RSSI	01/07/2026	Rédaction
Sammy SAHNOUNE	DSI	03/08/2026	Validation
Damien ROUSSET	Directeur Général Délégué	28/08/2026	Approbation

Historique des modifications		
Date de création	Version	Commentaires
20/02/2019	V0.0	Version de travail
21/10/2019	V1.0	Version intermédiaire
04/06/2020	V1.1	Version finale
01/07/2026	V1.2	Version révisée

Documents de référence			
Référence	Version	Date	Titre
La Politique de Sécurité des Systèmes d'Information de L'État	V1.0	23/09/2015	PSSI-E

1. Objectif de la PSSI Générale

L'objectif principal de la PGSSI est d'énumérer les grands principes de sécurité des systèmes d'information et qui sont déclinés dans les PSSIs Administrative et Recherche de l'INSERM.

Ce document définit les principes directeurs permettant d'élaborer les objectifs de sécurité des systèmes d'information des structures administratives et de recherche de l'INSERM qui sont formalisés dans les PSSIs administrative et recherche.

Cette PGSSI doit être validée, et rentrera en application le jour de sa publication.

Cette politique doit être revue à minima tous les ans ; au besoin, suite à :

- Un contrôle, résultats d'audits ou d'analyses de risques.
- Un changement important, en termes d'organisation, évolution technologique ou de la réglementation.
- Un incident important survenu sur le Système d'Information.

En cas de changement important, cette PSSI changera de version majeure. Une simple révision pour clarification ou ajustement entraînera un changement de version mineure.

2. Périmètre d'application de la PSSI

La présente PSSI s'applique à l'ensemble du périmètre des systèmes d'information de l'INSERM.

Les systèmes d'Information incluent l'ensemble des informations, processus et échanges informationnels, entre entités, afin que ces dernières accomplissent leurs fonctions dans le cadre du service qu'elles doivent délivrer. Toutes les parties prenantes de l'INSERM s'inscrivent donc dans le cadre des systèmes d'Information et doivent, par ailleurs, se conformer aux principes de cette PGSSI et le cas échéant aux règles des PSSI administratives et/ou recherche.

Le périmètre de la présente PGSSI regroupe le périmètre des systèmes d'information des structures administratives ainsi que des structures de recherche.

Le périmètre des structures administratives regroupe le siège central de l'INSERM, en ce compris les services de l'ANRS-MIE, ainsi que les délégations régionales de l'INSERM.

Le périmètre des structures de recherche regroupe essentiellement les structures de recherche de l'INSERM. Ce périmètre peut également concerner les personnels des délégations régionales de l'INSERM ou du Département des Systèmes d'Information en ce qu'ils sont amenés à faire application des règles de gestion des SI des structures de recherche dans le cadre des services SI fournis à ces dernières.

3. Principes directeurs de la PGSSI

Cadre SSI des politiques de sécurité des systèmes d'information de l'INSERM.

Afin de se mettre en conformité avec la PSSI-E, la politique générale de sécurité des systèmes d'information cadre les principes directeurs permettant d'assurer une cohérence d'ensemble au regard des objectifs de sécurité déclinés dans les PSSI administratives et recherche.

A la lecture de ces principes, ces derniers définissent la stratégie suivie au sein de l'INSERM afin d'assurer la sécurité des systèmes d'information.

Ces principes généraux sont les suivants :

- L'INSERM dimensionne et met en œuvre les moyens humains et financiers nécessaires afin de répondre aux enjeux de la sécurité.
- L'INSERM sécurise ses principaux actifs (ex : Méthodologies, travaux de recherche avant leurs publications, inventions et brevets, moyens de financement ...).
- L'INSERM sécurise les données à caractère personnel et attache une attention particulière aux données sensibles (ex : séquences ADN, dossiers médicaux, actes de décès ...).
- L'INSERM tend vers une haute disponibilité et une meilleure accessibilité aux services informatiques afin de favoriser l'innovation et la recherche.
- Avant toute mise en œuvre d'un système, L'INSERM s'assure de la conformité et la sécurité de ce système.
- Chaque utilisateur des ressources informatiques mises à sa disposition par l'INSERM doit être sensibilisé et informé de ses droits et devoirs.
- Afin de protéger son système d'information, l'INSERM doit mettre en œuvre les mesures techniques de protection nécessaires.
- Dans le cas où l'INSERM ferait appel à des prestations pour mettre en œuvre des systèmes d'information, celui-ci veillera au respect des exigences de sécurité relatives à la relation avec les tiers.
- L'INSERM utilise des moyens d'authentification adéquats robustes et proportionnels aux besoins de sécurité afin de gérer les accès aux ressources.
- L'INSERM trace et contrôle toute opération liée à la gestion et à l'administration du Système d'Information.
- Les administrateurs des systèmes d'information de l'INSERM adoptent les bonnes règles d'hygiène informatique dans le cadre de leurs fonctions.
- Quand cela répond à son besoin, l'INSERM met en œuvre des produits qualifiés par l'ANSSI pour assurer la sécurité de son Système d'Information.
- Toute information de nature sensible doit être hébergée sur le territoire national.

4. Chaîne fonctionnelle de la sécurité

Organisation de l'application et du suivi des politiques de sécurité des systèmes d'information de l'INSERM.

Afin de veiller à la bonne application des PSSI administrative et de recherche de l'INSERM, celui-ci se dote d'une chaîne fonctionnelle de pilotage de la Sécurité adaptée à sa structure.

Cette chaîne s'insère dans le dispositif décrit dans la PSSI-E au niveau des tutelles de l'INSERM.

Cette chaîne est la suivante :

- Le PDG de l'INSERM est l'Autorité Qualifiée en Sécurité des Systèmes d'Information. Il définit la Politique de Sécurité des Systèmes d'Information et est responsable vis-à-vis des ministères de tutelle du respect de celle-ci et des réglementations.
- Le PDG est assisté d'un Responsable de la Sécurité des Systèmes d'Information, qu'il nomme et mandate pour définir et veiller à la bonne réalisation et application de cette PSSI.
- Le PDG est assisté d'un Fonctionnaire Sécurité Défense, qui veille à la compatibilité de cette PSSI avec les objectifs de la Protection du Potentiel Scientifique et Technique de la Nation.
- Le RSSI est assisté dans les diverses régions administratives de l'INSERM par des Responsables des Systèmes d'Information. Ces derniers sont nommés par le Délégué Régional des régions concernées.
- Le RSSI et les RSI s'appuient pour le pilotage de la PSSI en local sur des Correspondants Sécurité du Système d'Information pour chaque entité de l'INSERM : Siège, ANRS-MIE, Délégations Régionales, structures de recherche labellisées INSERM.
- Le CSSI du Siège est nommé par l'Administrateur du Siège.
- Le CSSI de l'ANRS-MIE est nommé par le Directeur de l'ANRS-MIE.
- Le CSSI de chaque Délégation Régionale est nommé par le Délégué Régional. Il est la même personne que le RSI.
- Le CSSI de chaque structure de recherche INSERM est nommé par le Directeur de structure.
- Les CSSI s'appuient sur les moyens locaux ou nationaux pour la réalisation des objectifs de la PSSI sur leur périmètre.