La science pour la santé
From science to health

INSERM

Politique des Systèmes d'Information de Recherche V1.1

Politique de Sécurité du Système d'information v1.

Identification du document

Identification du document		
Document	**Sujet**	**Version du document**
PSSI	Politique de Sécurité des Systèmes d'Information de Recherche	V1.1

Approbation du document			
Nom	**Fonction**	**Date**	**Action**
TADJADIT	Consultant		Rédaction
CHAMBI	Chef de projet	21/10/2019	Validation
ARCHER	RSSI	04/06/2020	Validation
SAHNOUNE	DSI		Validation
GIRY	Directrice Générale Déléguée		Approbation

Historique des modifications			
Date de création	**Date d'application**	**Version**	**Commentaires**
20/02/2019	N/A	V0.0	Version de travail
21/10/2019	N/A	V1.0	Version finale
04/06/2020	?	V1.1	Version finale

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

Table des matières

1. Objectif de la PSSI recherche

L'objectif principale est de formaliser les règles de sécurité des systèmes d'information des structures recherche de l'INSERM.

La présente PSSI recherche formalise les pratiques SSI en vigueur et les objectifs à respecter pour renforcer le niveau de sécurité des systèmes d'information des Unités de recherche ou d'autres formations de recherche ou d'appui à la recherche de l'INSERM.

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

Cette politique doit être revue à minima tous les trois 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 réglementations.
- 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 entrainera un changement de version mineure.

2. Périmètre d'application de la PSSI

La présente PSSI s'applique à l'ensemble du périmètre des système d'information des structures de recherche 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 du Système d'Information et doivent, par ailleurs, se conformer aux règles de cette PSSI.

Ce périmètre concerne les unités de recherche ou d'autres formations de recherche ou d'appui à la recherche de l'INSERM. Ce périmètre peut également concerner les personnels des délégations régionales de l'INSERM ou du Département des Systèmes d'Information par rapport aux règles de gestion des SI des unités de recherche ou d'autres formations de recherche ou d'appui à la recherche.

Il appartient aux parties prenantes concernées d'assurer une cohérence entre les dispositions de la présente PSSI recherche et de la décliner au regard de leurs contextes.

Les unités de recherche ou d'autres formations de recherche ou d'appui à la recherche ayant des besoins particuliers en termes de sécurité du SI sont susceptible de déployer des PSSI spécifiques à leur contexte. Ces PSSI spécifiques doivent être compatibles a minima avec cette PSSI-Recherche, et éventuellement, les PSSI des autres tutelles- tutelles de l'unité de recherche, tutelles de la formation de recherche, ou d'appui à la recherche. Notamment, chaque PSSI spécifique doit être vérifiée lors de toute évolution de la PSSI-Recherche de l'INSERM, et éventuellement ajustée si besoin, dans un délai d'un an à compter de la nouvelle parution.

Un plan d'action doit être élaboré et mis en œuvre afin de se mettre en conformité avec les modalités de cette PSSI ou de toute PSSI spécifique.

3. Corps de la PSSI

Politique de sécurité des systèmes d'information des structures de recherche conforme avec la PSSI-E.

Afin de se mettre en conformité avec la PSSI-E, la politique de sécurité des systèmes d'information des structures de recherche de l'INSERM sera déclinée ci-dessous au regard de 34 objectifs de la PSSI-E.

Toute exception à une règle de la présente politique doit faire l'objet d'une dérogation, justifiée par le demandeur et validée par le RSSI. Les risques liés à la non mise en œuvre d'une règle doivent être pleinement acceptés par le demandeur.

3.1. Politique, organisation, gouvernance

3.1.1.Organisation de la SSI

Organisation SSI	**Identifiant:**	**ORG-SSI**

L'INSERM a désigné une organisation SSI composée de :

- Une Autorité Qualifiée de la Sécurité des Systèmes d'Informations (AQSSI), représentée par le Président Directeur Général de l'INSERM, il a comme responsabilité d'organiser la sécurité de l'information au sein de l'Inserm.
- Un fonctionnaire de sécurité défense (FSD) disposant d'une responsabilité transverse qui a la charge de protéger les connaissances et résultats de la recherche scientifique, ainsi que les technologies sensibles.
- Un Directeur du Département des Systèmes d'Informations qui a la responsabilité nationale de mise en œuvre, de la sécurisation et de la continuité de service du système d'information.
- Un Responsable Sécurité du Système d'Information (RSSI). Il est chargé de l'application de la présente politique de sécurité. Il est également responsable de la rédaction et du maintien à jour de la présente PSSI
- Un Responsable Sécurité du Système d'Information adjoint, en soutien au Responsable Sécurité du Système d'Information dans ses fonctions et qui le remplace en cas d'absence.
- Un délégué à la protection des données personnelles (DPO)
- Des chargés régionaux de la sécurité des systèmes d'information.
- Des correspondants de la sécurité des systèmes d'information dans les structures.

Il convient de nommer un correspondant SSI dans chaque structure de recherche. Ce dernier aura la responsabilité de piloter la sécurité du SI de la structure de recherche.

Il convient si possible que le correspondant SSI ait des compétences en informatique s'il effectue également la mise en œuvre de la SSI. Si possible, il convient de proposer des formations en sécurité informatique.

Identification des acteurs SSI	**Identifiant:**	**ORG-ACT-SSI**

L'INSERM a formellement identifié les acteurs SSI :

- Une Autorité Qualifiée de la Sécurité des Systèmes d'Informations (AQSSI) représenté par le PDG de l'INSERM
- Un Directeur du Département des Systèmes d'Informations
- Un Responsable Sécurité du Système d'Information (RSSI) dans la chaîne SSI.
- Un Responsable Sécurité du Système d'Information Adjoint
- Des Chargés régionaux de la sécurité des systèmes d'informations
- Des Correspondants locaux de la sécurité des systèmes d'informations

Il convient comme indiqué dans la partie organisation SSI (ORG-SSI) de nommer un correspondant informatique dans chaque unité de recherche.

L'INSERM à mis en place l'identification des différents acteurs SSI sur les fiches de postes sur la partie administrative.

Il convient de mettre en place l'identification des différents correspondant SSI des structures de recherche sur les fiches de poste de celle-ci.

Il convient que les responsabilités des correspondants SSI soient définis et mis à jour.

Désignation du responsable SSI	**Identifiant:**	**ORG-RSSI**

L'INSERM a formellement identifié l'Autorité Qualifiée de la Sécurité du Système d'Information (AQSSI) représenté par le PDG de l'INSERM ainsi qu'un Responsable Sécurité du Système d'Information (RSSI), un Responsable Sécurité du Système d'Information Adjoint et des chargés régionaux SSI.

Ces différents acteurs participent à garantir la sécurité de l'information, leurs rôles et responsabilités sont clairement définis et mises à jour.

Il convient que les correspondant SSI des structures de recherche effectuent des remontés d'informations vers les chargés régionaux de sécurité SI.

Gestion contractuelle des tiers	**Identifiant:**	**ORG-TIERS**

L'INSERM a défini les modalités d'accès aux informations et aux ressources informatiques, celle-ci sont soumises à des clauses de sécurité standards et spécifiques contenu dans les conventions avec les tiers.

L'INSERM exige formellement un plan d'assurance qualité et de sécurité (PAQ/PAS) dans les Cahiers des clauses techniques particulières (CCTP).

Il convient de satisfaire aux mêmes exigences dans les différentes structures de recherche gérées par l'INSERM.

Il convient que dans l'ensemble des structures de recherche gérées par l'INSERM les cahiers de clauses techniques particulières (CCTP) soient élaborés prenant en compte la SSI et signés par les prestataires et intervenants externes.

Définition et pilotage de la PSSI	**Identifiant:**	**ORG-PIL-PSSIM**

L'INSERM a formellement nommé un responsable pour la rédaction et le maintien à jour de la présente PSSI. Cette dernière définit l'ensemble des mesures de sécurité applicables au Système d'Information de l'INSERM

Il convient que ces mesures répondent aux différents chapitres, objectifs et règles issues de la PSSI. Il convient qu'elle soit applicable et qu'elle puisse s'adapter au besoin de sécurité de chaque unité de recherche.

Il convient de planifier, mettre en œuvre, contrôler et améliorer la présente politique de sécurité pour toutes les structures de recherche.

Application de l'instruction dans l'entité	**Identifiant:**	**ORG-APP-INSTR**

L'INSERM par l'intermédiaire des correspondants SSI planifient les actions de mise en application de la présente PSSI et les chargés régionaux de sécurité SI suivent la mise en œuvre de chaque plan d'action.

Il convient que ces actions soient mises à jour à la validation d'une nouvelle PSSI.

Il convient que les correspondants SSI des structures de recherche produisent un bilan annuel de sécurité afin de rendre compte de la mise en œuvre de la PSSI, suivant un modèle commun.

Il convient que les correspondants SSI des structures de recherche rendent compte de la mise en application des mesures ainsi qu'un état des lieux sur la sécurité des systèmes d'informations auprès du RSSI par l'intermédiaire de leur chargé régional de la SSI.

Formalisation de documents d'application	**Identifiant:**	**ORG-APP-DOCS**

L'INSERM décline les mesures de la PSSI en modalités et procédures d'application afin de garantir leur mise en œuvre.

Il convient de compléter les modalités et les procédures d'application de la PSSI et de les mettre à jour.

Il convient que ces modalités et procédures soient disponibles et applicables à l'ensemble des structures de recherche gérées par l'INSERM.

3.2. Ressources humaines

3.2.1. Ressources humaines

Charte d'application SSI	**Identifiant:**	**RH-SSI**

L'INSERM dispose d'une charte de bon usage des moyens informatiques en langue française et anglaise. Cette dernière est communiquée et est accessible via l'intranet aux nouveaux entrants.

Cette charte est sous la responsabilité directe du directeur des systèmes d'information (DSI). Celle-ci doit être lu, signée et approuvée par le personnel des structures de recherche pour les accès à tous les SI de l'INSERM, locaux ou distants.

L'INSERM fait référence à la charte informatique dans le règlement intérieur.

Choix et sensibilisation des personnes tenant les postes clés de la SSI	**Identifiant:**	**RH-MOTIV**

Il convient que l'INSERM en collaboration avec le RSSI propose un parcours de formation adapté aux correspondant SSI de l'ensemble des structures de recherche et élabore des compagnes de sensibilisation à destination des administrateurs SI, afin de formaliser les bonnes pratiques SSI en termes d'administration.

Il convient que les administrateurs des SI de l'ensemble des structures de recherche soient régulièrement sensibilisés à la SSI.

Personnels de confiance	**Identifiant:**	**RH-CONF**

Il convient que les structures de recherche gérées par l'INSERM imposent des clauses de confidentialité et de non divulgation aux acteurs liés hiérarchiquement ou fonctionnellement au SI.

Il convient que les personnes manipulant des données à caractère sensible soient identifiées.

Sensibilisation des utilisateurs des SI	**Identifiant:**	**RH-UTIL**

L'ensemble des structures de recherche gérées par l'INSERM doivent élaborer des campagnes de sensibilisation ponctuelles spécifiques à destination des utilisateurs de leur SI.

Il convient que les campagnes de sensibilisation soient régulières.

Il convient au RSSI de multiplier les efforts de communication sur les risques et attaques SSI (Phishing, Spam, …) de manière ponctuelle et que les correspondant SSI relaient ces informations afin de sensibiliser les utilisateurs à la sécurité du système d'information (SSI).

Gestion des arrivées, des mutations et des départs	**Identifiant:**	**RH-MOUV**

L'ensemble des structures de recherche gérées par l'INSERM doivent disposer de procédure formalisée de gestion des arrivées, des mutations et des départs des collaborateurs dans les SI.

Il convient que les structures de recherche disposent d'une procédure de gestion des habilitations pour les nouveaux arrivants.

Il convient de mettre à jour la procédure de gestion des arrivées, des mutations et des départs des structures de recherche de l'INSERM ainsi que de contribuer à son amélioration.

Gestion du personnel non permanent (stagiaires, intérimaires, prestataires…)	Identifiant:	RH-NPERM

Les structures de recherche gérées par L'INSERM doivent appliquer les règles de sécurité relatives au personnel non permanent au même titre que le personnel permanent.

La charte de bon usage des moyens informatiques et la PSSI sont communiquées à ces derniers.

3.3. Gestion des biens

3.3.1. Cartographie des SI

Inventaire des ressources informatiques	Identifiant:	GDB-INVENT

Il convient que l'ensemble des structures de recherche gérées par l'INSERM établissent un inventaire de leurs ressources informatiques et qu'il soit régulièrement maintenu à jour et si possible remonté au chargé régional de la sécurité SI.

Il convient que l'inventaire dispose d'une liste des "briques" matérielles et logicielles utilisées, ainsi que leurs versions exactes.

Il convient d'inclure dans l'inventaire, la configuration à jour de toutes les ressources informatiques.

Cartographie	Identifiant:	GDB-CARTO

Il convient à l'ensemble des structures de recherche gérées par l'INSERM de disposer d'une cartographie, précisant les centres informatiques (ex : salle machine, salle de sauvegarde) et si possible les architectures des réseaux. Il convient d'identifier les points névralgiques des réseaux dans la cartographie. Cette dernière doit être tenue à jour de manière annuelle.

Il convient d'élaborer une matrice de sensibilité en fonction de la cartographie des biens établies.

3.3.2. Qualification et protection de l'information

Qualification des informations	Identifiant:	GDB-QUALIF-SENSI

Il convient de définir et de formaliser une échelle de sensibilité approprié des informations traitées et que celles-ci soient évaluées.

Il convient de marquer systématiquement, tous les documents produits ou rédigés dans les structures de recherche gérées par l'INSERM en fonction de leur niveau de sensibilité.

Protection des informations	Identifiant:	GDB-PROT-IS

Les utilisateurs de l'ensemble des structures de recherche gérées par l'INSERM doivent posséder des anti-virus sur leurs postes de travail.

Il convient si possible de chiffrer les postes de travail et d'utiliser des disques amovibles chiffrés.

3.4. Intégration de la SSI dans le cycle de vie des systèmes d'information

3.4.1.Risques

Homologation de sécurité des systèmes d'information	Identifiant:	INT-HOMOLOG-SSI

Il convient que les structures de recherche gérées par l'INSERM disposent d'une procédure permettant de s'assurer que chaque système fasse l'objet d'une revue de sécurité, au préalable, avant sa mise en exploitation.

Il convient de formellement désigner une autorité locale pour l'élaboration des analyses de risques.

Il convient de concevoir, formaliser et mettre en œuvre une démarche d'homologation. Cette démarche devra inclure un dossier d'homologation en fonction des besoins de sécurité du système. Ce dossier est organisé et validé par une commission d'homologation. L'homologation sera prononcée au regard des éléments constituant ce dossier. La commission d'homologation, ainsi que l'autorité d'homologation, devront être définis par la structure.

3.4.2.Maintien en condition de sécurité

Intégration de la sécurité dans les projets	**Identifiant:**	**INT-SSI**

Il convient que l'ensemble des structures de recherche gérée par L'INSERM par l'intermédiaire des correspondant SSI intègre la sécurité dans toutes les phases du cycle de vie d'un projet informatique au travers de clauses de sécurité.

Il convient si possible de définir et de formaliser une méthodologie permettant d'atteindre les objectifs de sécurité.

Mise en œuvre au quotidien de la SSI	**Identifiant:**	**INT-QUOT-SSI**

L'ensemble des structures de recherche gérées par l'INSERM doit disposer d'une procédure d'hygiène informatique qui fait référence au guide de l'ANSSI.

Il convient de la mettre en œuvre afin de garantir la sécurité dans toutes les phases du cycle de vie d'un projet informatique, de sa conception jusqu'à son décommissionnement.

Créer un tableau de bord SSI	**Identifiant:**	**INT-TDB**

Il convient si possible que les structures de recherche gérées par l'INSERM disposent d'un tableau de bord SSI permettant de suivre l'application des règles de la présente PSSI, et d'allouer les moyens nécessaires, conformément à la règle (CONTR-SSI).

Ce tableau de bord doit être remonté aux responsables régionaux de manière régulière.

3.4.3.Produits et services qualifiés ou certifiés

Acquisition de produits et services de confiance	**Identifiant:**	**INT-AQ-PSL**

Les structures de recherche gérées par L'INSERM doivent faire référence à la liste des produits qualifié par l'ANSSI, lors de l'expression d'un besoin pour les projets sensibles.

En cas d'absence de qualification d'un produit par l'ANSSI, l'INSERM s'appuie sur le référentiel « Critères Commun ».

Le RSSI peut tenir à jour une liste de produits non qualifiés par l'ANSSI mais approuvés pour utilisation dans les projets sensibles. Les structures de recherche sont invitées à utiliser préférentiellement les produits de cette liste lorsque le produit qualifié n'existe pas.

Il convient, en cas d'utilisation d'un produit non qualifié pour un projet sensible, d'en informer le RSSI.

3.4.4.Maîtrise des prestations

Clauses de sécurité	**Identifiant:**	**INT-PRES-CS**

La structure de recherche gérée par l'Inserm doit inclure des clauses de sécurité standards et spécifiques dans le cadre des conventions avec les tiers.

Il convient de spécifier avec les tiers les mesures SSI que tout prestataire intervenant sur les SI des structures de recherche s'engage à respecter dans le cadre de ses interventions.

Suivi et contrôle des prestations fournies	**Identifiant:**	**INT-PRES-CNTRL**

L'ensemble des structures de recherche gérées par l'INSERM doit réaliser des audits lorsque le niveau de sécurité d'un projet est très sensible.

Il convient afin de maintenir un niveau de sécurité adéquat que le correspondant SSI de la structure de recherche, mène des contrôles périodiques sur les actions du sous-traitant pour vérifier leur conformité au cahier des charges. Les prestataires se doivent de fournir un compte-rendu de leurs actions menées à l'issue de chaque intervention, et ces comptes-rendus doivent être conservés.

Il convient que la structure de recherche gérée par l'Inserm effectue périodiquement des contrôles pour s'assurer du bon respect des clauses mises en place dans (INT-PRES-CS).

Analyse de risques	**Identifiant:**	**INT-REX-AR**

Il convient de disposer d'une méthodologie de gestion de risques au sein des structures de recherche gérées par l'INSERM.

Il convient également d'appliquer à toute opération d'externalisation cette méthodologie de gestion de risques, dans le but de formaliser les objectifs de sécurité et de définir les mesures de sécurité adéquates.

Hébergement	**Identifiant:**	**INT-REX-HB**

Il convient que l'ensemble des structures de recherche gérées par l'INSERM identifie clairement ses données sensibles.

L'hébergement de celle-ci doit être réalisé dans les conditions réglementaires applicables.

Il convient d'effectuer une sauvegarde des données sensibles.

Hébergement et clauses de sécurité	**Identifiant:**	**INT-REX-HS**

L'ensemble des structures de recherche gérées par L'INSERM doit utiliser des solutions d'hébergement adéquates.

Il convient que les solutions d'hébergement soient clairement identifiées au sein des structures de recherche et remontées aux responsables régionaux.

3.5. Sécurité physique

3.5.1. Sécurité physique des locaux abritant les SI

Découpage des sites en zones de sécurité	**Identifiant:**	**PHY-ZONES**

Il convient si possible de découper chaque structure de recherche en plusieurs zones physiques suivant le niveau de sécurité nécessaire.

Il convient également que leur plan soit régulièrement à jour.

Accès réseau en zone d'accueil du public	**Identifiant:**	**PHY-PUBL**

Il convient, quand une unité de recherche ou une formation de recherche ou d'appui à la recherche dispose d'une zone publique, de la séparer de la zone professionnelle.

Il convient de retirer l'accès au réseau d'une unité de recherche de la zone publique, ou de cloisonner physiquement ce réseau (ex : prises RJ45). Il convient si possible que les bornes wifi de l'ensemble des structures de recherche donnent accès uniquement à l'internet via un réseau séparé de son réseau interne.

Protection des informations sensibles au sein des zones d'accueil	Identifiant:	PHY-SENS

Il est interdit de traiter les informations sensibles au niveau des zones d'accueil du public

Sécurité physique des locaux techniques	Identifiant:	PHY-TECH

Les locaux techniques au sein des structures de recherche contenant les équipements d'alimentation du réseau et de téléphonie doivent être protégés. L'accès aux boites de connexion internet du réseau de données doit être sécurisé.

Les accès aux armoires de brassages doivent être sécurisés a minima par clé.

Il convient que les accès aux salles de serveurs des structures de recherche soient protégés a minima par une clé.

Il convient que le personnel non informatique soit encadré lors de sa présence dans les salles serveurs.

Il convient que les correspondants SSI des structures de recherche garde une trace des possesseurs de clés ou autres moyens d'accès pour chacun des locaux décrits plus haut.

Protection des câbles électriques et de télécommunications	Identifiant:	PHY-TELECOM

Il convient que le câblage réseau des structures de recherche gérées par l'INSERM soit protégé contre les dommages et les interceptions de communications.

Les panneaux de raccordements et les salles de câbles doivent être situés en dehors des zones d'accueil.

Il convient que l'accès à ces panneaux et ces salles soit contrôlé et si possible que soit identifié les intervenants.

Contrôles anti-piégeages	Identifiant:	PHY-CTRL

Il convient que l'ensemble des structures de recherche gérées par L'INSERM effectue des opérations de contrôle du matériel afin de vérifier toute présence de matériel ou logiciel non légitime (ex : keylogger, sniffer réseau…).

3.5.2.Sécurité physique des centres informatiques

Découpage des locaux en zones de sécurité	**Identifiant:**	**PHY-CI-LOC**

L'ensemble des structures de recherche doit être découpé en zones physiques de sécurité tel décrit dans (PHY-TECH).

Convention de service en cas d'hébergement tiers	**Identifiant:**	**PHY-CI-HEBERG**

En cas de mutualisation de l'hébergement, il convient qu'une convention de service entre les tiers, définissant les responsabilités mutuelles en matière de sécurité soit définie.

Contrôle d'accès physique	**Identifiant:**	**PHY-CI-CTRLACC**

Un contrôle d'accès physique doit être mis en place aux zones restreintes, tel décrit dans (PHY-TECH).

Délivrance des moyens d'accès physique	**Identifiant:**	**PHY-CI-MOYENS**

L'ensemble des unités de recherche gérées par l'INSERM doit disposer d'une procédure permettant de délivrer le moyen d'accès aux locaux.

Il convient si possible de mettre en place une procédure permettant de s'assurer de l'identité des personnes accédant aux locaux.

Il convient également de mettre en place une procédure d'identification des visiteurs.

Traçabilité des accès	**Identifiant:**	**PHY-CI-TRACE**

Les structures de recherche gérée par l'INSERM doivent disposer d'une procédure de traçabilité des accès par les visiteurs externes aux zones sécurisées.

Il convient que les motifs des accès aux zones sécurisées soient clairement établis.

Il convient de garder les traces d'accès des visiteurs aux locaux pendant un an.

Il convient de garder les traces d'accès aux zones restreintes pendant un an.

Local énergie	Identifiant:	PHY-CI-ENERGIE

L'alimentation secteur des équipements doit être conforme aux règles de l'art.

Il convient de faire vérifier annuellement les équipements par un prestataire spécialisé.

Ce dernier doit fournir d'un compte-rendu formel.

Climatisation	Identifiant:	PHY-CI-CLIM

Les structure de recherche doivent mettre en place des dispositifs de climatisation dans les salles machines le justifiant.

Des procédures et des vérifications annuelles des climatiseurs doivent être mises en place.

Il convient si possible que les climatiseurs, possèdent une sonde de déclenchement forcé et un capteur de température.

Lutte contre l'incendie	Identifiant:	PHY-CI-INC

Des dispositifs matériels de protection contre le feu doivent être installés dans l'ensemble des locaux techniques.

Il convient que ces équipements soient mis aux normes de manière régulière par un organisme certifié.

Il convient que les correspondant SSI des structures de recherche veillent à la propreté des locaux techniques de leur périmètre et interdise le dépôt de cartons, papiers ou autre source potentielle de départ de feu.

Il convient d'effectuer périodiquement une procédure de test d'évacuation en cas d'incendie. Il convient également d'effectuer régulièrement des vérifications sur le fonctionnement des extincteurs.

Lutte contre les voies d'eau	Identifiant:	PHY-CI-EAU

Il convient de mener une étude des risques liée aux voies d'eau.

Il convient également que cette étude prenne en compte le risque de fuite d'eau douce.

3.6. Sécurité des réseaux

3.6.1. Usage sécurisé des réseaux nationaux

Systèmes autorisés sur le réseau	**Identifiant:**	**RES-MAITRISE**

Il convient de limiter le plus possible la connexion au réseau local des équipements non gérés et non configurés par les équipes informatiques dans l'ensemble des structures de recherche gérées par l'INSERM.

Les équipements non gérés par les équipes informatiques doivent être considérés comme présentant un risque élevé et, dans la mesure du possible, être confinés sur des réseaux spécifiques.

Interconnexion avec des réseaux externes	**Identifiant:**	**RES-INTERCO**

L'ensemble des structures de recherche de l'INSERM doit s'assurer du contrôle des interconnexions de réseaux externes.

Il convient que les liaisons avec internet soient protégées.

Mettre en place un filtrage réseau pour les flux sortants et entrants	**Identifiant:**	**RES-ENTSOR**

Un filtrage des connexions sensibles depuis l'extérieur vers le réseau local de chaque unité de recherche gérées par l'INSERM doit être réalisé.

Il convient si possible que le filtrage soit réalisé à l'aide d'un pare-feu.

Protection des informations	**Identifiant:**	**RES-PROT**

Il convient que l'ensemble des structures de recherche gérées l'INSERM sensibilise son personnel sur l'importance du chiffrement d'information.

Il convient que soit formalisée une procédure de chiffrement d'information à destination d'internet.

3.6.2. Usage sécurisé des réseaux locaux

Cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes	**Identifiant:**	**RES-CLOIS**

Les structures de recherche gérée par l'INSERM doivent disposer d'un SI, si possible segmenté en zones de sécurité homogènes.

3.6.3.Accès spécifiques

Interconnexion des sites géographiques locaux d'une entité	**Identifiant:**	**RES-INTERCOGEO**

Il convient de sécuriser et de contrôler les interconnexions de réseaux locaux.

Cloisonnement des ressources en cas de partage de locaux	**Identifiant:**	**RES-RESS**

Il convient que les ressources informatiques soient cloisonnées physiquement ou logiquement entre les différentes entités en cas de partage des locaux.

Cas particulier des accès spécifiques dans une entité	**Identifiant:**	**RES-INTERNET-SPECIFIQUE**

Les cas d'accès spécifiques doivent être contrôlés et justifiés.

Il convient à l'INSERM d'interdire la prise en main à distance sans autorisation explicite et de l'acter par le correspondant SSI, au cas par cas suivant le besoin, ponctuel ou récurrent.

3.6.4.Usage sécurisé des réseaux sans fil

Mise en place de réseaux sans fil	**Identifiant:**	**RES-SSFIL**

Il convient d'effectuer une analyse de risque des réseaux sans fil.

Il convient de généraliser des mécanismes de chiffrement et d'authentification.

Il convient d'effectuer la segmentation des réseaux afin de limiter la surface d'attaque.

3.6.5.Sécurité des mécanismes de commutation et de routage

Implanter des mécanismes de protection contre les attaques sur les couches basses	**Identifiant:**	**RES-COUCHBAS**

Il convient si possible d'utiliser des mécanismes de protection des couches basses (ex : le filtrage d'adresses mac, les protections contre l'ARP spoofing).

Surveiller les annonces de routage	**Identifiant:**	**RES-ROUTDYN**

Lorsqu'il existe des routages dynamiques au sein des structures de recherche gérées par l'INSERM, il convient que les annonces de ces routages soient surveillées.

Modifier systématiquement les éléments d'authentification par défaut des équipements et services	**Identifiant:**	**RES-SECRET**

Il convient de changer tous les mots de passes par défaut des équipements des SI et de changer également les certificats installés par défaut.

Durcir les configurations des équipements de réseaux	**Identifiant:**	**RES-DURCI**

Il convient que les interfaces et services inutiles soient systématiquement désactivés afin de durcir la configuration des équipements réseaux.

Il convient d'établir un plan de contrôle et de conformité de la configuration de ces équipements.

3.6.6.Cartographie réseau

Élaborer les documents d'architecture technique et fonctionnelle	**Identifiant:**	**RES-CARTO**

Il convient que chaque structure de recherche dispose d'une architecture réseau de son SI.

Il convient que la cartographie réseau soit régulièrement mise à jour.

Il convient si possible d'intégrer la configuration des équipements aux schémas de l'architecture réseau et de mettre en place des mesures adéquates afin de protéger ses documents.

3.7. Architecture des SI

3.7.1. Architecture sécurisée des centres informatiques

Principes d'architecture de la zone d'hébergement	Identifiant:	ARCHI-HEBERG

Il convient si possible de mettre en œuvres des zones démilitarisées (DMZ) afin de cloisonner et protéger les services accessibles depuis l'extérieur.

Des VLAN doivent si possible être mis en place afin de segmenter les LAN en sous-réseaux isolés.

Il convient si possible que Les flux applicatifs et d'administration soient séparés et filtrés.

Architecture de stockage et de sauvegarde	Identifiant:	ARCHI-STOCKCI

Il convient de disposer d'une architecture dédiée au stockage et à la sauvegarde des données.

Passerelle Internet	Identifiant:	ARCHI-PASS

Il convient de disposer d'un mécanisme de filtrage au niveau de la passerelle Internet.

3.8. Exploitation des SI

3.8.1. Protection des informations sensibles

Protection des informations sensibles en confidentialité et en intégrité	Identifiant:	EXP-PROT-INF

Il convient de chiffrer de manière systématique les informations sensibles à l'aide de moyens de chiffrement labellisés afin de préserver leurs confidentialité et intégrité.

3.8.2.Surveillance et configuration des ressources informatiques

Traçabilité des interventions sur le système	**Identifiant:**	**EXP-TRAC**

Il convient de mettre en place un registre des interventions de maintenance des ressources informatique à minima sur format papier.

Il convient que ce registre soit conservé à des fins de preuve et reste accessible au correspondant SSI pendant au moins un an.

Il convient également de relever les motifs d'accès au système.

Configuration des ressources informatiques	**Identifiant:**	**EXP-CONFIG**

Les structures de recherche doivent si possible appliquer un durcissement des systèmes d'exploitation et des logiciels sur l'ensemble de leurs SI.

Il convient de démarrer une procédure de mise à jour des systèmes d'exploitation dès la parution d'une nouvelle mise à jour de sécurité.

Il convient de mettre à jour l'ensemble des logiciels sur les serveurs et postes de travail de la structure de recherche dans le cadre du maintien en condition de sécurité. Ces modalités doivent faire l'objet d'un suivi selon un processus formalisé.

Documentation des configurations	**Identifiant:**	**EXP-DOC-CONFIG**

Il convient de réaliser un inventaire documenté des ressources informatiques.

Il convient que cette documentation soit mise à jour à chaque changement notable.

3.8.3.Autorisations et contrôles d'accès

Identification, authentification et contrôle d'accès logique	**Identifiant:**	**EXP-ID-AUTH**

L'authentification de tout utilisateur ayant accès aux ressources non publiques doit être exigé.

Il convient si possible d'utiliser un mécanisme d'authentification forte pour accéder aux données qualifiées très sensibles.

La structure de recherche doit définir et formaliser un processus de gestion des droits d'accès en adéquation avec la gestion des arrivées, des mutations et des départs des utilisateurs du SI.

Droits d'accès aux ressources	Identifiant:	EXP-DROITS

Il convient de définir une échelle de sensibilité spécifique ainsi que le besoin de diffusion et de partage des ressources.

Il convient si possible que l'ensemble des structures de recherche puisse disposer d'une liste traçant les droits d'accès aux données pour chaque individu.

Il convient que les utilisateurs disposent de droits d'accès aux seules ressources dont ils ont besoin dans le cadre de leur travail.

Gestion des profils d'accès aux applications	Identifiant:	EXP-PROFILS

Au sein des structures de recherche gérées par L'INSERM doivent être mis en place des mécanismes permettant de limiter les services, les données et les privilèges auxquels ont accès les utilisateurs en fonction de leurs rôles et responsabilités. Ces mécanismes reposent sur l'attribution d'identifiants et de moyens d'authentification aux différentes applications.

Il convient aux structures de recherche de définir et de mettre à jour la liste des profils utilisateurs ayant accès aux données très sensibles.

Autorisations d'accès des utilisateurs	Identifiant:	EXP-PROC-AUTH

Il convient de formaliser un processus d'autorisation gérant les accès utilisateurs aux ressources des SI et de faire dans ce processus la distinction entre les utilisateurs permanents et les utilisateurs de courte durée.

Il convient de mettre en adéquation ce processus avec la politique de gestion des RH (RH-MOUV).

Revue des autorisations d'accès	Identifiant:	EXP-REVUE-AUTH

Il convient que les correspondants SSI dressent un inventaire des autorisations d'accès au sein de leur structure et qu'ils puissent revoir périodiquement l'implémentation de ces droits d'accès à minima tous les ans.

Confidentialité des informations d'authentification	Identifiant:	EXP-CONF-AUTH

Les informations d'authentifications doivent être considérées comme des données sensibles.

Il convient de ne pas les partager et de les chiffrer en local.

Gestion des mots de passe	Identifiant:	EXP-GEST-PASS

Il est interdit de stocker les mots de passe en clair sur les postes de travail.

Il est interdit le stockage des mots de passe sur supports papier (post-it).

Il convient si possible d'utiliser des protocoles chiffrés permettant de ne pas diffuser en clair les mots de passe sur le réseau.

Il convient également que les mots de passe des postes utilisateurs et administrateurs soit gérés par une politique de mots de passe.

Initialisation des mots de passe	Identifiant:	EXP-INIT-PASS

Il convient de changer les mots de passe lors de la première utilisation du poste de travail.

Politique des mots de passe	Identifiant:	EXP-POL-PASS

L'ensemble des structures de recherche doit respecter à minima les règles de gestion et de protection de mots de passe de l'INSERM.

Il convient de contrôler périodiquement, à minima tous les ans, les paramètres techniques relatifs aux mots de passe.

La politique des mots de passe exige l'utilisation de :

- 8 caractères pour les postes locaux
- 12 pour les ressources à distance (applications par exemple) avec caractères spéciaux

Utilisation de certificats électroniques	Identifiant:	EXP-CERTIFS

Au sein des structures de recherche de l'INSERM l'application des règles techniques du RGS doit être un prérequis pour l'utilisation des certificats électroniques.

Contrôle systématique de la qualité des mots de passe	Identifiant:	EXP-QUAL-PASS

Ce processus doit être en adéquation avec la politique des mots de passe (EXP-POL-PASS).

Séquestre des authentifiant « administrateur »	Identifiant:	EXP-SEQ-ADMIN

Les authentifiant permettant l'administration des ressources doivent être placés sous séquestre à minima papier. Ceux-ci doivent être tenus à jour.

La structure doit mettre en place des mécanismes permettant de tracer et d'identifier les personnes ayant des accès d'administration aux ressources informatiques.

En application du RGPD, il convient que les administrateurs des systèmes d'information soient informés des finalités des traitements manipulant leurs informations personnelles.

Politique de mots de passe « administrateurs »	**Identifiant:**	**EXP-POL-ADMIN**

Chaque administrateur au sein des structures de recherche doit disposer d'un mot de passe distinct et destiné exclusivement à l'administration.

Gestion du départ d'un administrateur des SI	**Identifiant:**	**EXP-DEP-ADMIN**

En cas de départ d'un administrateur, les comptes de cet administrateur doivent être désactivés.

Il convient de gérer ces comptes en adéquation avec la politique de gestion des RH (RH-MOUV).

3.8.4.Sécurisation de l'exploitation

Restriction des droits	**Identifiant:**	**EXP-RESTR-DROITS**

Il convient que les utilisateurs ayant des droits d'administration aient un compte administrateur distinct de leur compte utilisateur habituel.

Protection des accès aux outils d'administration	**Identifiant:**	**EXP-PROT-ADMIN**

Il convient si possible de mettre en place une procédure formelle d'autorisation d'accès aux outils d'administration.

Il convient que les outils et interfaces d'administration des SI soient limités aux personnes habilitées.

Habilitation des administrateurs	**Identifiant:**	**EXP-HABILIT-ADMIN**

L'habilitation des administrateurs doit s'effectuer selon une procédure validée par le directeur de structure.

Gestion des actions d'administration	Identifiant:	EXP-GEST-ADMIN

Il convient si possible de tracer les opérations d'administration dans l'ensemble des structures de recherche.

Sécurisation des flux d'administration	Identifiant:	EXP-SEC-FLUXADMIN

Il convient si possible d'utiliser des protocoles sécurisés (ex : SSH, HTTPS) pour administrer les ressources locales.

Un sous-réseau doit être si possible dédié à l'administration et doit être séparé logiquement des opérations d'utilisations du SI.

Il convient de séparer logiquement les sessions utilisateur des sessions administrateur afin de garantir une ségrégation de ces fonctions.

Sécurisation des outils de prise de main à distance	Identifiant:	EXP-SECX-DIST

Les structures de recherche doivent disposer d'un moyen de prise en main à distance sécurisé si elles en ont le besoin.

L'ensemble des structures de recherche doit définir le périmètre des opérations de prise en main à distance et doivent l'interdire sans autorisation explicite.

Définir une politique de gestion des comptes du domaine	Identifiant:	EXP-DOM-POL

Il convient de réaliser et de suivre une politique documentée de gestion des comptes du domaine quand la structure de recherche dispose d'un domaine active directory.

Configurer la stratégie des mots de passe des domaines	Identifiant:	EXP-DOM-PASS

Une complexité minimale dans le choix des mots de passe doit être imposée aux différents utilisateurs afin notamment de limiter les attaques par brute force.

La stratégie des mots de passe des domaines est mise en adéquation avec la politique des mots de passe (EXP-POL-PASS).

Définir et appliquer une nomenclature des comptes du domaine	Identifiant:	EXP-DOM-NOMENCLAT

Il convient que les identifiants des comptes soient reconnaissables selon leur type (utilisateur standard, administration, compte de service).

Restreindre au maximum l'appartenance aux groupes d'administration du domaine	Identifiant:	EXP-DOM-RESTADMIN

Il convient de limiter le plus possible l'appartenance aux groupes d'administration.

Maîtriser l'utilisation des comptes de service	Identifiant:	EXP-DOM-SERV

La structure de recherche doit tenir un inventaire permettant de répertorier l'ensemble des comptes de service ainsi que les applications et systèmes les utilisant.

Il convient de formaliser et mettre en place une procédure permettant de changer les mots de passe de ces comptes en urgence.

Limiter les droits des comptes de service	Identifiant:	EXP-DOM-LIMITSERV

Il convient que les comptes de service suivent le principe du moindre privilège concernant les droits d'accès.

Désactiver les comptes du domaine obsolètes	Identifiant:	EXP-DOM-OBSOLET

Il convient de supprimer ou de désactiver les comptes utilisateurs au plus tard un an après leur obsolescence dans l'ensemble des structures de recherche gérées par l'INSERM.

Améliorer la gestion des comptes d'administrateur locaux	Identifiant:	EXP-DOM-ADMINLOC

Il convient de définir une politique de gestion des comptes d'administration locaux. Il convient que cette politique impose un mot de passe diffèrent sur chaque machine.

Maintenance externe	Identifiant:	EXP-MAINT-EXT

Il convient de déterminer quelle sont les données sensibles afin d'appliquer le traitement adéquat aux ressources.

Il convient d'effacer les données non chiffrées de toute ressource informatique avant l'envoi en maintenance externe.

Il convient d'utiliser des produits qualifiés pour effacer les données sensibles.

Mise au rebut	Identifiant:	EXP-MIS-REB

Les données présentes sur les disques durs doivent être effacées de manière adéquate lorsqu'une ressource informatique (poste, support, serveurs, nomades, mobiles) est amenée à quitter définitivement une structure de recherche.

Il convient si possible d'effectuer l'effacement des données sensibles avec des produits qualifiés et certifiés.

Protection contre les codes malveillants	**Identifiant:**	**EXP-PROT-MALV**

Tous les équipements vulnérables de l'ensemble des unités de recherche gérées par l'INSERM doivent être équipés de logiciels antivirus à jour.

Gestion des événements de sécurité de l'antivirus	**Identifiant:**	**EXP-GES-ANTIVIR**

Il convient de centraliser et de corréler les évènements antivirus.

Mise à jour de la base de signatures	**Identifiant:**	**EXP-MAJ-ANTIVIR**

Il convient de déployer les mises à jour d'antivirus automatiquement et systématiquement sur l'ensemble des équipements des SI.

Configuration du navigateur Internet	**Identifiant:**	**EXP-NAVIG**

Il convient de configurer de manière sécurisée le navigateur Internet déployé sur les SI de l'ensemble des structures de recherche gérées par l'INSERM (ex : Des services inutiles, nettoyage du magasin de certificats, …) grâce à une configuration type.

Définir et mettre en œuvre une politique de suivi et d'application des correctifs de sécurité	**Identifiant:**	**EXP-POL-COR**

Il convient qu'une politique de suivi et d'application des correctifs de sécurité soit définie et appliquée dans les structures de recherche gérées par l'INSERM.

Déploiement des correctifs de sécurité	**Identifiant:**	**EXP-COR-SEC**

Il convient que les correctifs de sécurités soient déployés régulièrement sur les SI par les structures de recherche gérées par l'INSERM.

Assurer la migration des systèmes obsolètes	Identifiant:	EXP-OBSOLET

Il convient que les versions des logiciels utilisés soient tenues à jour et que le support soit assuré par l'éditeur ou à défaut de les isoler du réseau.

Isoler les systèmes obsolètes restants	Identifiant:	EXP-ISOL

Des systèmes obsolètes au sein des SI de certaines structures de recherche gérées par l'INSERM peuvent, de manière exceptionnelle, être gardés volontairement pour assurer la continuité opérationnelle des projets.

Il convient si possible dans l'ensemble des structures de recherche gérées par l'INSERM d'isoler au niveau du réseau, des éléments d'authentification et des applications, les systèmes obsolètes du SI de l'INSERM.

Journalisation des alertes	Identifiant:	EXP-JOUR-SUR

L'ensemble des structures de recherche gérées par l'INSERM doit mettre en place des dispositifs de journalisation pour chaque système.

Définir et mettre en œuvre une politique de gestion et d'analyse des journaux de traces	Identifiant:	EXP-POL-JOUR

Il convient que les structures de recherche gérées par l'INSERM disposent d'une politique de gestion et d'analyse des journaux et que le personnel concerné en soit informé.

Conservation des journaux	Identifiant:	EXP-CONS-JOUR

Il convient que les journaux des évènements de sécurité soient conservés sur 12 mois.

3.8.5.Défense des systèmes d'information

Gestion dynamique de la sécurité	Identifiant:	EXP-GES-DYN

Il convient si possible que les structures de recherche gérées par l'INSERM analysent les journaux de sécurité.

Il convient également que l'équipe en charge de la SSI analyse les flux réseaux entrants/sortants.

Maîtrise des matériels	Identifiant:	EXP-MAIT-MAT

L'ensemble des structures de recherche gérées par l'INSERM doit éviter la connexion d'équipements non maîtrisés, non administrés et non mis à jour par l'INSERM, aux différents équipements de son parc informatique.

Rappel des mesures de protection contre le vol	Identifiant:	EXP-PROT-VOL

Il convient que tous les postes fixes de l'ensemble des structures de recherche gérées par l'INSERM soit protégé physiquement contre le vol à minima par un câble anti-vol.

Il convient également que les supports amovibles soient chiffrés et stockés dans des endroits sûrs.

Déclarer les pertes et vols	Identifiant:	EXP-DECLAR-VOL

Il convient de déclarer aux correspondant SSI lorsqu'il y a un vol d'une ressource des SI.

Ceux-ci

Réaffectation de matériels informatiques	Identifiant:	EXP-REAFFECT

Il convient de formaliser et de mettre en place une procédure de gestion du matériels informatiques en adéquation avec la politique de gestion des RH (RH-MOUV).

Il convient d'inclure à cette procédure des mesures d'effacement sécurisées des données.

Déclaration des équipements nomades aptes à traiter des informations sensibles	Identifiant:	EXP-NOMAD-SENS

Il convient que les équipements nomades traitant des informations sensibles fassent l'objet d'une homologation de la part du directeur de la structure de recherche.

Accès à distance au système d'information de l'organisme	Identifiant:	EXP-ACC-DIST

L'accès à distance au SI des structures de recherche doit s'effectuer par l'utilisation d'un VPN chiffré nécessitant une authentification.

Impression des informations sensibles	Identifiant:	EXP-IMP-SENS

Il convient de mettre en place une procédure concernant l'impression des informations sensibles dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient si possible que l'impression requiert une authentification de l'utilisateur.

Sécurité des imprimantes et copieurs multifonctions	**Identifiant:**	**EXP-IMP-2**

Il convient de protéger les imprimantes physiquement dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient de limiter les services des imprimantes au strict minimum.

3.8.6. Exploitation sécurisée des centres informatiques

Systèmes d'exploitation	**Identifiant:**	**EXP-CI-OS**

Les systèmes d'exploitation déployés dans l'ensemble des structures de recherche gérées par l'INSERM doivent faire l'objet d'un support valide de la part de leur éditeur.

Il convient que seuls les services et les applications nécessaires soient installés, de façon à réduire la surface d'attaque.

Il convient qu'un contrôle d'accès avec des droits d'administration restreints soit appliqué sur ces services.

Logiciels en Tiers Présentation	**Identifiant:**	**EXP-CI-LTP**

Il convient que la configuration des logiciels déployés en tiers présentation au sein de l'ensemble des structures de recherche gérées par l'INSERM soit renforcée.

Logiciels en Tiers Application	**Identifiant:**	**EXP-CI-LTA**

Il convient que les logiciels en tiers application fassent l'objet d'un développement sécurisé dans l'ensemble des structures de recherche.

Logiciels en Tiers Données	**Identifiant:**	**EXP-CI-LTD**

Il convient que l'ensemble des structures de recherche gérées par l'INSERM appliquent des règles très strictes aux logiciels en tiers données.

Passerelle d'échange de fichiers	**Identifiant:**	**EXP-CI-PROTFIC**

Il convient d'utiliser des protocoles sécurisés et à jour pour l'ensemble des échanges de fichiers entre les applications.

Messagerie technique	**Identifiant:**	**EXP-CI-MESSTECH**

Il convient afin de satisfaire les besoins d'exploitation et de supervision des infrastructures et applications, de déployer une messagerie technique au sein du SI de l'ensemble des structures de recherche gérées par L'INSERM.

Filtrage des flux applicatifs	**Identifiant:**	**EXP-CI-FILT**

Il convient que des mécanismes de filtrage de flux et de cloisonnement des flux applicatifs soient mises en place pour protéger les SI de l'ensemble des structures de recherche gérées par l'INSERM contre les attaques informatiques.

Flux d'administration	**Identifiant:**	**EXP-CI-ADMIN**

Il convient que les flux d'administration système soient séparés si possible des flux d'administration applicatifs et qu'ils soient protégés via un mécanisme de cloisonnement logique (ex : VLAN).

Il convient également que l'attribution des droits d'administration respecte cette différenciation.

Effacement de support	**Identifiant:**	**EXP-CI-EFFAC**

Il convient de formaliser les procédures d'effacement des disques dur pour permettre leur réutilisation et reconditionnement dans l'ensemble des structures de recherche gérées par l'INSERM.

Destruction de support	**Identifiant:**	**EXP-CI-DESTR**

Une procédure de destruction ou d'effacement sécurisée des supports de stockages des matériels doit être appliquée avant la mise au rebut.

Il convient de formaliser une clause dans les contrats avec les sous-traitants de matériel (telles les imprimantes en location) pour s'assurer que le sous-traitant procède de manière sécurisée à l'effacement des données.

Traçabilité / imputabilité	Identifiant:	EXP-CI-TRAC

Il convient afin d'assurer une cohérence dans les échanges entre applications et une traçabilité pertinente des évènements techniques que le service NTP soit utilisé dans l'ensemble des équipements des SI des structures de recherche gérées par l'INSERM.

Supervision	Identifiant:	EXP-CI-SUPERVIS

Il convient que les flux de supervision (ex : remontée d'informations) et les flux d'administration (ex : commandes, mises à jour) au sein des structures de recherche gérées par l'INSERM soient cloisonnés, si possible.

Accès aux périphériques amovibles	Identifiant:	EXP-CI-AMOV

Il convient que l'accès aux périphériques amovibles fasse l'objet d'un traitement adapté.

Accès aux réseaux	Identifiant:	EXP-CI-ACCRES

Il convient que les opérations de gestion des accès aux réseaux (contrôle physique des accès, attribution des adresses IP, filtrage des informations) soient soumises à des procédures sécurisées dans l'ensemble des structures de recherche gérées par l'INSERM.

.

Audit/contrôle	Identifiant:	EXP-CI-AUDIT

Il convient que l'ensemble des structures de recherche gérées par l'INSERM puisse effectuer des audits sur leur SI conformément aux règles (CONTR-SSI, CONTR-BILAN-SSI).

3.9. Sécurité du poste de travail

3.9.1. Sécurisation des postes de travail

Fourniture et gestion des postes des travail	Identifiant:	PDT-GEST

Il convient si possible que les postes de travail fixes, nomades et mobiles du personnel permanent soient fournis et gérés par l'équipe locale chargée des SI dans l'ensemble des structures de recherche gérées par l'INSERM.

Formalisation de la configuration des postes des travail	Identifiant:	PDT-CONFIG

Il convient qu'une procédure de configuration des postes de travail soit formalisée dans l'ensemble des structures de recherche.

Verrouillage de l'unité centrale des postes fixes	Identifiant:	PDT-VEROUIL-FIXE

Il convient que les postes fixes soient protégés par des systèmes antivols dans l'ensemble des structures de recherche gérées par l'INSERM.

Verrouillage des postes portables	Identifiant:	PDT-VEROUIL-PORT

Il convient que la fourniture des câbles physiques de sécurité soit obligatoire dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient de sensibiliser les utilisateurs à leur utilisation.

Réaffectation du poste de travail	Identifiant:	PDT-REAFFECT

Il convient qu'une procédure de sécurité soit mise en place dans l'ensemble des structures de recherche qui décrit les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés.

Privilèges des utilisateurs sur les postes de travail	Identifiant:	PDT-PRIVIL

Il convient que le principe des moindres privilèges soit appliqué pour les droits utilisateurs aux utilisateurs des SI sur tous les postes de travail dans l'ensemble des structures de recherche gérées par l'INSERM.

Utilisation des privilèges d'accès « administrateur »	Identifiant:	PDT-PRIV

Il convient que les privilèges d'accès "administrateur" soient utilisés uniquement pour les actions d'administration le nécessitant et soient distincts des comptes individuels dans l'ensemble des structures de recherche gérées par l'INSERM.

Gestion du compte « administrateur local »	Identifiant:	PDT-ADM-LOCAL

Il convient que l'accès aux comptes administrateurs des postes fixes soit limité autant que possible aux équipes SI dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient également qu'un mot de passe différent soit utilisé pour chaque administrateur local.

Stockage des informations	**Identifiant:**	**PDT-STOCK**

Il convient que les données traitées par les utilisateurs soient préférentiellement stockées sur des espaces réseaux.

Il convient que la sauvegarde des données soit effectuée à intervalle régulier.

Il convient de rappeler aux utilisateurs de stocker l'ensemble des données sensibles sur l'espace réseau sécurisé.

Sauvegarde / Synchronisation des données locales	**Identifiant:**	**PDT-SAUV-LOC**

Il convient dans le cas où des données sont stockées en local sur les postes que des moyens de synchronisation ou de sauvegarde soient fournis aux utilisateurs dans l'ensemble des structures de recherche gérées par l'INSERM.

Partage de fichiers	**Identifiant:**	**PDT-PART-FIC**

Il convient afin de limiter les surfaces d'attaque et de divulgation des données en interne, que L'INSERM interdise systématiquement le partage de répertoires ou de fichiers hébergés localement sur les postes de travail dans l'ensemble des structures de recherche gérées par l'INSERM.

Suppression des données sur les postes partagés	**Identifiant:**	**PDT-SUPPR-PART**

Il convient que les données présentes sur les postes partagés soient effacées entre deux utilisations dans l'ensemble des structures de recherche gérées par l'INSERM.

Chiffrement des données sensibles	**Identifiant:**	**PDT-CHIFF-SENS**

Il convient que les données sensibles sur l'ensemble des postes de travail et supports amovibles soient chiffrées.

Il convient de chiffrer l'ensemble des données sensibles sur les serveurs utilisés au sein des structures de recherche.

Il convient également d'utiliser des outils de chiffrement labellisés afin d'assurer au mieux la protection de ces données.

Fourniture de supports de stockage amovibles	Identifiant:	PDT-AMOV

Il convient que des supports de stockage amovibles (ex : clés USB et disque durs externes) soient fournis aux utilisateurs du SI de l'INSERM en fonction des besoins de leurs activités.

Il convient d'interdire les connexions des terminaux amovibles personnel dans l'ensemble des structures de recherche.

Accès à distance aux Systèmes d'Information de l'entité	Identifiant:	PDT-NOMAD-ACCESS

Afin de maîtriser la sécurité, les accès à distance aux SI de l'ensemble des structures de recherche gérées par l'INSERM doivent être réalisés via leur infrastructure.

Il convient si possible que dans les cas d'utilisations d'autres infrastructures, l'utilisation d'un VPN soit protégée par un moyen d'authentification.

Pare-feu local	Identifiant:	PDT-NOMAD-PAREFEU

Il convient d'installer un pare-feu local sur les équipements nomades des SI de l'ensemble des structures de recherche gérées par l'INSERM.

Stockage local d'information sur les postes nomades	Identifiant:	PDT-NOMAD-STOCK

Il convient que le stockage d'information sur les postes nomades soit limité au strict nécessaire dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient que les informations sensibles de tous les postes nomades soient chiffrées afin d'en protéger leur confidentialité.

Filtre de confidentialité	Identifiant:	PDT-NOMAD-FILT

Il convient si possible de fournir des filtres de confidentialités pour les postes nomades manipulant des données sensibles.

Configuration des interfaces de connexion sans fil	Identifiant:	PDT-NOMAD-CONNEX

Il convient de durcir la configuration des interfaces sans fil afin de limiter les usages malveillants dans l'ensemble des structures des recherche gérées par l'INSERM.

Il convient également de formaliser des règles de configuration de la carte réseau.

Désactivation des interfaces de connexion sans fil	Identifiant:	PDT-NOMAD-DESACTIV

Il convient si possible de désactiver les interfaces sans fil (ex : Wifi, Bluetooth, 3G…) non utilisées sur les postes de travail de l'ensemble des structures de recherche gérées par l'INSERM.

Il convient d'activer ces interfaces uniquement en cas de besoin et de les configurer selon un guide de configuration sécurisé, afin de limiter les intrusions.

3.9.2.Sécurisation des copieurs multifonctions

Durcissement des imprimantes et copieurs multifonctions	Identifiant:	PDT-MUL-DURCISS

Il convient que tous les mots de passe par défaut des équipements soient changés dès leur mises en fonctions dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient que toutes les interfaces et services inutiles soient désactivées et que l'espace de stockage de données soit chiffré, si possible.

Sécurisation de la fonction de numérisation	Identifiant:	PDT-MUL-SECNUM

Afin de sécuriser au mieux la fonction de numérisation des documents, l'envoi de documents à destination d'adresses de messageries internes doit être limité à une seule adresse de messagerie à la fois dans l'ensemble des structures de recherche gérées par l'INSERM.

3.9.3.Sécurisation de la téléphonie

Sécuriser la configuration des autocommutateurs	Identifiant:	PDT-TEL-MINIM

Il convient de privilégier la téléphonie sur IP (TOIP).

Il convient lorsqu'une unité de recherche dispose d'autocommutateurs de les maintenir à jour au niveau des correctifs de sécurité.

Codes d'accès téléphoniques	Identifiant:	PDT-TEL-CODES

Il convient que les messageries vocales soient toutes protégées par un mot de passe à code pin dans l'ensemble des structures de recherche gérées par l'INSERM.

Limiter l'utilisation du DECT	Identifiant:	PDT-TEL-DECT

Il convient que l'utilisation du DECT (téléphone sans fil) soit restreinte.

Il convient de formaliser les dérogations pour l'utilisation des DECT au sein des structures de recherche de l'INSERM.

Attribution des accès téléphoniques	Identifiant:	PDT-TEL-INSERM

Il convient que les équipements téléphoniques soient alloués à une personne ou une salle en particulier si possible dans l'ensemble des unités de recherche gérées par l'INSERM.

3.9.4. Contrôles de la conformité des postes de travail

Utiliser des outils de vérification automatique de la conformité	Identifiant:	PDT-CONF-VERIF

Il convient d'établir un planning d'inventaires de configurations de postes de travail dans l'ensemble de structures de recherche gérées par l'INSERM.

Il convient de procéder à des inventaires de configurations de postes de travail à minima tous les ans.

Il convient si possible de le faire à l'aide d'un outil spécialisé.

Il convient que cet outil puisse vérifier l'homogénéité des postes de travail entre eux, et de vérifier les programmes installés sur ces derniers.

3.10. Sécurité du développement des systèmes

3.10.1. Prise en compte de la sécurité dans le développement des SI

Intégrer la sécurité dans les développements locaux	**Identifiant:**	**DEV-INTEGR-SECLOC**

Afin d'intégrer la sécurité dans les projets de développement, en collaboration avec les partenaires il convient de mettre en place le cas échéant des mesures de sécurité à partir de l'étape de conception jusqu'à son retrait (analyse des risques sur le système, plan d'assurance sécurité, protection des actifs liés au projet, formation et sensibilisation, bonnes pratiques de développement sécurisé, durcissement, plan de tests, audits, revue de code et scans de vulnérabilités, …) dans l'ensemble des structures de recherche gérées par l'INSERM.

Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique	**Identifiant:**	**DEV-SOUS-TRAIT**

Il convient de formaliser des exigences de sécurités dans l'ensemble des unités de recherche gérées par l'INSERM. Les partenaires doivent s'engager par le plan d'assurance sécurité (PAS) à respecter les normes de développements sécurisées.

Les prestataires développeurs doivent produire de la documentation technique décrivant l'implémentation des protections développées (ex : Gestion de l'authentification, stockage des mots de passe, gestion des droits, chiffrement…).

Il convient d'imposer dans les contrats avec les prestataires la correction des vulnérabilités remontées, sous des délais convenables.

3.10.2. Prise en compte de la sécurité dans le développement des logiciels

Limiter les fuites d'information	**Identifiant:**	**DEV-FUITES**

La diffusion d'informations concernant les produits utilisés dans les logiciels doit être limité lors de l'intégration, de façon sécurisée afin de limiter les fuites d'informations et réduire les probabilités d'attaques externes dans l'ensemble des structures de recherche gérées par l'INSERM.

Réduire l'adhérence des applications à des produits ou technologies spécifiques	Identifiant:	DEV-LOG-ADHER

Il convient si possible de limiter au maximum les adhérences des applications à des environnements spécifiques afin de limiter les failles de sécurité et d'assurer le maintien des systèmes en condition de sécurité dans l'ensemble des structures de recherche gérées par l'INSERM.

Instaurer des critères de développement sécurisé	Identifiant:	DEV-LOG-CRIT

Il convient d'inclure dans le cahier des charges des critères de sécurisation pour les phases d'intégration pour les développeurs dans l'ensemble des structures de recherche gérées par l'INSERM.

Intégrer la sécurité dans le cycle de vie logiciel	Identifiant:	DEV-LOG-CYCLE

Il convient à la structure de recherche de disposer des règles de sécurité à suivre tout au long du cycle de vie des applications, de la phase de conception jusqu'à la phase de maintenance applicative.

Améliorer la prise en compte de la sécurité dans les développements Web	Identifiant:	DEV-LOG-WEB

Les développeurs travaillant pour les structures de recherche gérées par l'INSERM doivent respecter le top 10 OWASP (Open Web Application Security Project) afin de prendre en compte la sécurité dans les développements web.

Calculer les empreintes de mots de passe de manière sécurisée	Identifiant:	DEV-LOG-PASS

Il convient dans l'ensemble des structures de recherche gérées par l'INSERM d'utiliser différentes technologies de cryptologie afin de protéger les mots de passes stockés.

Les structure de recherche gérées par l'INSERM doivent mettre en place un mécanisme pour protéger les empreintes de mots de passes contre les attaques par force brute.

Mettre en œuvre des fonctionnalités de filtrage applicatif pour les applications à risque	Identifiant:	DEV-FILT-APPL

Il convient que l'ensemble des structures de recherche gérées par L'INSERM puisse disposer d'un filtrage en entrée des applications à risque.

3.11.Traitement des incidents

3.11.1 Chaînes opérationnelles

Chaînes opérationnelles SSI	**Identifiant:**	**TI-OPS-SSI**

Il convient de formaliser une procédure de traitement des incidents de sécurité dans l'ensemble des structures de recherche gérées par l'INSERM.

Il convient que cette procédure puisse inclure toutes les règles relatives à ce chapitre de la PSSI.

Il convient que cette procédure soit mise à jour et améliorée régulièrement.

Il convient de formaliser des procédures opérationnelles, accompagnées de fiches reflexes, décrivant la résolution de chaque type d'incident. Ces procédures doivent être maintenues à jour.

Mobilisation en cas d'alerte	**Identifiant:**	**TI-MOB**

Il convient que l'ensemble des structures de recherche gérées par L'INSERM formalise une procédure de traitement des incidents, dans laquelle figure l'organisation de la gestion des incidents (chaîne fonctionnelle et opérationnelle de traitement des incidents, points de contact et moyens de communication) ainsi que les mesures à prendre pour traiter les alertes de sécurité. La structure de recherche doit si possible disposer d'une plateforme de recueil des alertes et des incidents.

Qualification et traitement des incidents	**Identifiant:**	**TI-QUAL-TRAIT**

Dans la procédure de traitement des incidents, le sous-processus de qualification et de traitement des incidents de sécurité doit être mis en place (appréciation, classement et résolution des incidents par type) par l'intermédiaire d'un outil dans l'ensemble des structures de recherche gérées par l'INSERM.

La chaîne fonctionnelle SSI doit contribuer à la qualification de l'incident, à son pilotage et à son traitement. Le correspondant SSI pilote le traitement des risques.

Remontée des incidents	**Identifiant:**	**TI-INC-REM**

L'ensemble des structures de recherche gérées par l'INSERM doit maintenir à jour un historique clair des suites liées à l'escalade de chaque incident.

Il convient de formaliser, dans la procédure de traitement des incidents, le sous-processus de détection et remontée des incidents de sécurité (moyens de détection et de déclaration d'alertes et d'incidents).

Il convient de formaliser, dans la procédure de traitement des incidents, le processus de revue et analyse post-incident (historique des traitements des incidents, capitalisation et amélioration continue de ce processus).

3.12 Continuité d'activité

3.12.1 Gestion de la continuité d'activité

Définition du plan local de continuité d'activité des systèmes d'information	**Identifiant:**	**PCA-LOCAL**

Il convient que l'ensemble des structures de recherche gérées par l'INSERM puisse disposer d'un plan de continuité d'activité SI (PCI) local.

Le plan de continuité d'activité SI, formalise la structure ainsi que les attendus permettant d'assurer la continuité d'activité.

Suivi de la mise en œuvre du plan de continuité d'activité local des Systèmes d'Information (PCA des SI)	**Identifiant:**	**PCA-SUIVILOCAL**

Il convient que les correspondant SSI pilotent le plan de continuité d'activité SI (PCI).

Mise en œuvre des dispositifs techniques et des procédures opérationnelles	**Identifiant:**	**PCA-PROC**

Il convient que l'ensemble des structures de recherche gérées par L'INSERM instaure des moyens techniques de redondance au niveau de certains équipements très sensible.

Il convient que ces moyens techniques soient supervisés et maintenus dans le temps via des dispositifs de gestion de la capacité.

Il convient que l'ensemble des structures de recherche gérées par l'INSERM formalise ces dispositifs techniques dans le plan de continuité d'activité SI et rédige des procédures opérationnelles facilitant leur mise en œuvre.

Protection de la disponibilité des sauvegardes	Identifiant:	PCA-SAUVE

Il convient que les données sauvegardées soient répliquées si nécessaires.

Protection de la confidentialité des sauvegardes	Identifiant:	PCA-PROT

Il convient que les structures de recherche gérées par l'INSERM mettent en œuvre un contrôle d'accès aux données sauvegardées.

Pour les données très sensible l'absence de réplication doit être justifié.

Il convient de chiffrer si besoin ces sauvegardes afin d'en assurer l'intégrité et la confidentialité. Les clés de chiffrement doivent être adéquatement protégées.

Exercice régulier du plan local de continuité d'activité des systèmes d'information	Identifiant:	PCA-EXERC

Il convient que le plan de continuité d'activité soit testé régulièrement dans l'ensemble des structures de recherche gérées par l'INSERM. Il convient de définir les scénarios de tests et les exercices en fonction d'objectifs spécifiques à atteindre (test de revue documentaires, exercice de mise en situation, test des procédures d'alertes, simulation de situation de crise, …).

Mise à jour du plan local de continuité d'activité des systèmes d'information	Identifiant:	PCA-MISAJOUR

Il convient que le PCI soit régulièrement mis à jour (évolution du SI suite aux résultats de tests, changement organisationnel, …) dans l'ensemble des structures de recherche gérées par l'INSERM.

3.13 Conformité, audit, inspection, contrôle

3.13.1 Contrôles réguliers

Contrôles locaux	Identifiant:	CONTR-SSI

Il convient à l'ensemble des structures de recherche gérées par l'INSERM de mettre en œuvre des mesures de pilotage de la présente PSSI à l'aide de tableaux de bord de suivi.

Il convient si possible de réunir régulièrement un comité de pilotage (COPIL) chargé de suivre la mise en œuvre et le contrôle des règles de la PSSI.

Il convient si possible de mandater une équipe d'audit interne ou externe, indépendante de la DSI, afin de réaliser un audit de la mise en œuvre des règles de la présente PSSI, à minima tous les trois ans.

Bilan annuel	**Identifiant:**	**CONTR-BILAN-SSI**

Il convient de faire un bilan annuel dans l'ensemble des structures de recherche mesurant la maturité du SSI globale afin de rendre compte de la mise en œuvre de la PSSI-E.

Il convient de tenir un bilan annuel du niveau de maturité globale sur la base des contrôles locaux réalisés, en conformité avec la règle (CONTR-SSI).

4. Annexe

4.1. Exigences non retenues :

Sécurisation du SI de sûreté	**Identifiant:**	**PHY-SI-SUR**
L'INSERM ne dispose pas de SI de sûreté à ce jour. Si la structure en dispose, se référer à la PSSIE.		

Centraliser la gestion du système d'information	**Identifiant:**	**EXP-CENTRAL**
Il est difficile voire impossible de centraliser la gestion sur le périmètre des structures de recherche. Il convient si possible que chaque structure de rechercher s'auto administre.		

Configurer le protocole IGP de manière sécurisée	**Identifiant:**	**RES-ROUTDYN-IGP**
Il n'y a pas de protocole de routage dynamique en place au sein des structures de recherche gérées par l'INSERM.		

Sécuriser les sessions EGP	**Identifiant:**	**RES-ROUTDYN-EGP**
Il n'y a pas de protocole de routage dynamique en place au sein des structures de recherche gérées par l'INSERM.		

Définition du plan ministériel de continuité d'activité des Systèmes d'Information	**Identifiant:**	**PCA-MINIS**
L'INSERM ne dispose pas de PCA intégré au PCA ministériel pour l'instant. Un PCA global pour l'INSERM (communication, locaux…) ne traitant pas de la continuité informatique existe.		

Inserm

La science pour la santé
From science to health