La science pour la santé
From science to health

# INSERM

## Politique des Systèmes d'Information Administrative V1.1

## Politique de Sécurité du Système d'information v1.

# Identification du document

| Identification du document | | |
|---|---|---|
| **Document** | **Sujet** | **Version du document** |
| INSERM | Politique de Sécurité des Systèmes d'Information de l'Administration | V1.1 |

| Approbation du document | | | |
|---|---|---|---|
| **Nom** | **Fonction** | **Date** | **Action** |
| TADJADIT | Consultant | | Rédaction |
| CHAMBI | Chef de projet | 23/03/2019 | 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 |
| 23/03/2019 | N/A | V1.0 | Version intermédiaire |
| 04/06/2020 | N/A | 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 ..... 4
2. Périmètre d'application de la PSSI ..... 5
3. Corps de la PSSI ..... 6
   - 3.1. Politique, organisation, gouvernance ..... 7
     - 3.1.1. Organisation de la SSI ..... 7
   - 3.2. Ressources humaines ..... 9
     - 3.2.1. Ressources humaines ..... 9
   - 3.3. Gestion des biens ..... 11
     - 3.3.1. Cartographie des SI ..... 11
     - 3.3.2. Qualification et protection de l'information ..... 12
   - 3.4. Intégration de la SSI dans le cycle de vie des systèmes d'information ..... 12
     - 3.4.1. Risques ..... 12
     - 3.4.2. Maintien en condition de sécurité ..... 13
     - 3.4.3. Produits et services qualifiés ou certifiés ..... 14
     - 3.4.4. Maîtrise des prestations ..... 14
   - 3.5. Sécurité physique ..... 15
     - 3.5.1. Sécurité physique des locaux abritant les SI ..... 15
     - 3.5.2. Sécurité physique des centres informatiques ..... 16
   - 3.6. Sécurité des réseaux ..... 18
     - 3.6.1. Usage sécurisé des réseaux nationaux ..... 18
     - 3.6.2. Usage sécurisé des réseaux locaux ..... 19
     - 3.6.3. Accès spécifiques ..... 19
     - 3.6.4. Usage sécurisé des réseaux sans fil ..... 20
     - 3.6.5. Sécurité des mécanismes de commutation et de routage ..... 20
     - 3.6.6. Cartographie réseau ..... 21
   - 3.7. Architecture des SI ..... 22
     - 3.7.1. Architecture sécurisée des centres informatiques ..... 22
   - 3.8. Exploitation des SI ..... 22
     - 3.8.1. Protection des informations sensibles ..... 22
     - 3.8.2. Surveillance et configuration des ressources informatiques ..... 23
     - 3.8.3. Autorisations et contrôles d'accès ..... 24
     - 3.8.4. Sécurisation de l'exploitation ..... 26
     - 3.8.5. Défense des systèmes d'information ..... 31
     - 3.8.6. Exploitation sécurisée des centres informatique ..... 34
   - 3.9. Sécurité du poste de travail ..... 37
     - 3.9.1. Sécurisation des postes de travail ..... 37

3.9.2. Sécurisation des copieurs multifonctions ..... 40
3.9.3. Sécurisation de la téléphonie ..... 41
3.9.4. Contrôles de la conformité des postes de travail ..... 41
3.10. Sécurité du développement des systèmes ..... 42
3.10.1. Prise en compte de la sécurité dans le développement des SI ..... 42
3.10.2. Prise en compte de la sécurité dans le développement des logiciels ..... 43
3.11. Traitement des incidents ..... 44
3.11.1 Chaînes opérationnelles ..... 44
3.12. Continuité d'activité ..... 45
3.12.1. Gestion de la continuité d'activité ..... 45
3.13. Conformité, audit, inspection, contrôle ..... 47
3.13.1. Contrôles réguliers ..... 47
4. Annexe ..... 48
4.1. Exigences non retenues : ..... 48

# 1. Objectif de la PSSI administrative

L'objectif principale de la présente PSSI administrative est de formaliser les règles de sécurité des systèmes d'information des structures administratives de l'INSERM.

La présente PSSI formalise les pratiques SSI en vigueur et les objectifs à respecter pour renforcer le niveau de sécurité des systèmes d'information des structures administratives de l'INSERM.

Cette dernière doit être validée et rentrera en vigueur 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 systèmes d'information des structures administratives 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 règles de cette PSSI.

Le périmètre des structures administratives regroupe la direction générale de l'INSERM, les Instituts Thématiques, l'ANRS-maladies infectieuses émergentes, les départements ainsi que les délégations régionales.

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

Un plan d'action doit être élaboré et mis en œuvre afin de se mettre en conformité avec les modalités de cette PSSI. Ce plan d'action est piloté et mis en œuvre par le DSI de l'INSERM et le RSSI.

# 3. Corps de la PSSI

## *Politique de sécurité des systèmes d'information des structures administratives 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 administratives 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 fonctionnelle 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 des systèmes d'information (DSI) qui est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseau, systèmes de stockage, de sauvegarde et d'impression, etc.) et logiciels des systèmes d'information, ainsi que du choix et de l'exploitation des services de télécommunications mis en œuvre, au niveau national.
- Un Responsable Sécurité du Système d'Information (RSSI), il est chargé de la mise en œuvre et 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)
- De Chargés Régionaux de la Sécurité des Systèmes d'Information.

Le Département des Systèmes d'Information dispose d'une organisation dédiée à la SSI :

- Une « Cellule sécurité » s'occupant de la Sécurité du système d'information fonctionnelle
- Un service « Sécurité opérationnelle » s'occupant de l'application opérationnelle de la SSI et de la surveillance de celui-ci.

L'INSERM dispose de procédures formalisées de notifications et de contacts avec l'ANSSI.

La présente PSSI définit l'ensemble des mesures de sécurité applicables au Système d'Information de l'INSERM. Il convient de décliner ces mesures en modalités et procédures d'application afin de garantir leurs mises en œuvre.

| **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) qui est le PDG de l'INSERM
- Un Responsable Sécurité du Système d'Information (RSSI) dans la chaîne SSI
- Un Directeur du Département des Systèmes d'Informations
- Des Directeurs régionaux de la sécurité des systèmes d'informations
- Un Responsable Sécurité du Système d'Information Adjoint
- Des Chargés Régionaux de la Sécurité du Système d'Information

L'INSERM doit mettre en place l'identification des différents acteurs SSI sur les fiches de postes

Il convient que les responsabilités de ces acteurs soient définies et mis à jour.

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

L'INSERM à 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) et un Responsable Sécurité du Système d'Information Adjoint.

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

| **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 élabore des Cahiers de clauses techniques particulières prenant en compte la sécurité du SI, signés par les prestataires et intervenants externes.

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

| **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-E.

Il convient de planifier, mettre en œuvre, contrôler et améliorer la présente politique de sécurité.

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

L'INSERM par l'intermédiaire du RSSI planifie les actions de mise en application de la présente PSSI et suit la mise en œuvre de chaque plan d'action.

Il convient que ces actions soient mises à jour à la validation de la nouvelle PSSI.

L'INSERM par l'intermédiaire du RSSI produit un bilan annuel de sécurité afin de rendre compte de la mise en œuvre de la PSSI.

Il convient que le RSSI rende compte de la mise en application des mesures ainsi qu'un état des lieux sur la sécurité des systèmes d'informations auprès de son autorité qualifiée, ainsi qu'auprès des tutelles.

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

La PSSI décrit les objectifs de sécurité sous forme de mesures.

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

Il convient de tenir à jour les procédures d'application de la PSSI et de les mettre en œuvre dès que disponibles.

# 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 intranet aux utilisateurs.

Il convient de la mettre à jour régulièrement.

Cette charte est sous la responsabilité directe du directeur des systèmes d'information (DSI). Celle-ci doit être lue, signée et approuvée.

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 acteurs de l'organisation SSI, et élabore des compagnes de sensibilisation à destination des administrateurs SSI, afin de formaliser les bonnes pratiques SSI en termes d'administration.

Il convient que les administrateurs des SI soient régulièrement sensibilisés à la SSI.

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

Il convient que l'INSERM impose des clauses de confidentialité et de non divulgation aux acteurs rattachés hiérarchiquement ou fonctionnellement au DSI.

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

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

L'INSERM élabore des campagnes de sensibilisation ponctuelles en collaboration avec le RSSI à destination des utilisateurs du 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 afin de sensibiliser les utilisateurs à la sécurité du système d'information (SSI).

Il convient que les formations pour les applications métiers incluent une partie de sécurité.

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

L'INSERM possède une procédure RH formalisée de gestion des arrivées, des mutations et des départs des collaborateurs dans les SI.

Le RSSI de l'INSERM doit disposer d'une procédure de gestion des habilitations pour les nouveaux arrivants.

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

Les habilitations aux applications métiers ne sont pas centralisées actuellement. Ces dernières sont gérées directement au niveau de chaque application et dans les différents locaux de chaque SI de l'INSERM

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

L'INSERM fait appliquer les règles de sécurité au personnel non permanent au même titre que le personnel permanent.

Il convient de désigner un agent pour contrôler l'application des règles par le personnel non 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** |
|---|---|---|

L'INSERM doit établir un inventaire de ses ressources informatiques et de ses équipements gérés par l'administrateur et doit le maintenir régulièrement à jour.

Au sein de l'INSERM il existe une liste des "briques" matérielles et logicielles utilisées, ainsi que leurs versions exactes pour les postes de travail.

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

Il convient que ces deux inventaires soient tenus à jour régulièrement.

| **Cartographie** | **Identifiant:** | **GDB-CARTO** |
|---|---|---|

L'INSERM doit définir une cartographie, précisant les centres informatiques (salle machine, salle de sauvegarde), les architectures des réseaux et les architectures applicatives. Les points névralgiques des réseaux sont identifiés dans la cartographie. Cette dernière est tenue à jour au moins annuellement.

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

### 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 des informations traitées au sein des SI de l'INSERM. Les informations de l'INSERM doivent être évaluées vis-à-vis de cette échelle

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

| Protection des informations | Identifiant: | GDB-PROT-IS |
|---|---|---|

Les utilisateurs au sein de l'INSERM possèdent des anti-virus sur leurs postes de travail. Le chiffrement des postes de travail doit être systématique dans la mesure du possible.

Il convient d'utiliser le chiffrement des disques amovibles.

## 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 |
|---|---|---|

L'INSERM doit disposer 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 au sein de l'INSERM.

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 l'INSERM et peut varier suivant le système à homologuer. |

## 3.4.2.Maintien en condition de sécurité

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

L'INSERM par l'intermédiaire du RSSI intègre la sécurité dans toutes les phases du cycle de vie d'un projet informatique au travers des clauses de sécurité définies dans les CCTP.

Il convient 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'INSERM fait référence au guide de l'ANSSI en termes de pratique SSI d'hygiène informatique.

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

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

Il convient de disposer d'un tableau de bord SSI permettant de suivre l'application des règles de la présente PSSI au sein des structures administrative de l'INSERM, et d'allouer les moyens nécessaires, conformément à la règle (CONTR-SSI).

## 3.4.3.Produits et services qualifiés ou certifiés

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

L'INSERM doit faire référence à la liste des produits qualifiés 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 » pour évaluer de manière autonome la qualification du produit.

## 3.4.4.Maîtrise des prestations

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

L'INSERM doit inclure des clauses de sécurité standards et spécifiques dans le cadre des conventions avec les tiers. L'INSERM exige également un Plan d'Assurance Sécurité dans tous les CCTP lors des consultations.

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

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

L'INSERM doit réaliser des audits lorsque le niveau de sécurité d'un projet est jugé sensible.

Il convient afin de maintenir un niveau de sécurité adéquat que l'équipe SI de l'INSERM chargée d'encadrer les prestations, mène des contrôles périodiques sur les actions des sous-traitants pour vérifier leurs conformités aux cahiers des charges. Les prestataires de l'INSERM se doivent de fournir un compte-rendu de leurs actions menées à l'issue de chaque intervention et ces compte-rendu doivent être conservés.

Il convient que 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** |
|---|---|---|

Une méthodologie de gestion de risques au sein de L'INSERM doit être élaborée.

Il convient 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** |
|---|---|---|

Toutes les données administratives de l'INSERM doivent être stockées sur le territoire national.

Des copies de certains éléments de celles-ci peuvent être réalisées pour des besoins techniques sur le territoire de l'Union Européenne.

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

L'INSERM doit mettre en place des solutions d'hébergement dans les datacenters préconisés par le ministère chargé de la recherche.

# 3.5. Sécurité physique

## 3.5.1. Sécurité physique des locaux abritant les SI

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

Les locaux de l'INSERM doivent être découpés en plusieurs zones physiques de sécurité. Les bureaux sont séparés des datacenters, qui disposent d'une procédure d'autorisation spécifique pour les droits d'entrées.

Il convient cependant que leur plan soient régulièrement mis à jour.

Les bureaux DSI de l'INSERM disposent de serrures pouvant être fermées à clé.

| **Sécurité physique des locaux techniques** | **Identifiant:** | **PHY-TECH** |
|---|---|---|

Les locaux techniques du siège et des délégations régionales au sein de l'INSERM contenant les équipements d'alimentation, de serveurs, de réseau et de téléphonie doivent être protégés physiquement et contrôlés.

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

Le câblage réseau de l'INSERM doit être à minima de catégorie 5, il est gainé et protégé contre les dommages et les interceptions de communications dans tous les locaux de l'INSERM.

L'accès aux panneaux de raccordement de l'INSERM doit se faire par des agents clairement désignés et identifiés.

| **Contrôles anti-piégeages** | **Identifiant:** | **PHY-CTRL** |
|---|---|---|

L'INSERM doit effectuer des opérations de contrôle du matériel, à minima par le recensement des adresses MAC.

Il convient d'améliorer les opérations de contrôle du matériel, afin de vérifier toute présence de matériel ou logiciel non légitime (keylogger, sniffer réseau…).

## 3.5.2.Sécurité physique des centres informatiques

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

Les locaux de L'INSERM doivent être découpés en zones physiques de sécurité, tel décrit dans **PHY-TECH.**

L'INSERM doit disposer d'une convention de service entre les tiers, définissant les responsabilités mutuelles en matière de sécurité avec les datacenters nationaux et Les hébergeurs externes.

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

L'INSERM doit disposer de conventions de services avec les tiers, définissant les responsabilités mutuelles en matière de sécurité entre le datacenter nationaux et des hébergeurs externes.

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

L'INSERM doit disposer d'un contrôle d'accès physique par badge aux zones de sécurité, tel décrit dans **PHY-TECH.**

Une procédure de renouvellement de contrôle d'accès aux zones sécurisés doit être mise en place de manière régulière et systématique.

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

L'INSERM doit disposer d'une procédure permettant de demander un badge pour les accès aux locaux.

Il convient de mettre en place une procédure qui permet de s'assurer de l'identité des personnes accédant aux locaux.

Il convient également de mettre en place un système d'identification des visiteurs.

La sécurité des accès physiques aux datacenters nationaux doit être qualifiée du niveau de zones à régime restrictif et doit être de la responsabilité de ces derniers.

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

Les administrateurs de l'INSERM ont accès aux zones sécurisées notamment à la salle serveur.

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

Il convient de garder des traces d'accès des visites au sein des locaux pendant un an.

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

| Local énergie | Identifiant: | PHY-CI-ENERGIE |
|---|---|---|

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

Il convient de faire vérifier annuellement les équipements par un prestataire spécialisé. Ce dernier doit fournir un compte-rendu écrit.

| Climatisation | Identifiant: | PHY-CI-CLIM |
|---|---|---|

L'INSERM doit 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 au sein de l'INSERM.

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 au sein de l'INSERM. Les salles machines ainsi que les locaux techniques doivent disposer de moyens matériels de protection contre les incendies.

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

Il convient de veiller à la propreté de l'ensemble des locaux techniques de l'INSERM. Il est interdit le dépôt de cartons, papiers ou autre source potentielle de départ de feu.

L'INSERM doit effectuer périodiquement une procédure de test d'évacuation en cas d'incendie. Elle effectue 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 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** |
|---|---|---|

L'INSERM interdit formellement et techniquement par l'intermédiaire du filtrage MAC au personnel de se connecter au réseau local avec des équipements non supervisés et non configurés par les équipes informatiques.

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

L'INSERM par l'intermédiaire de l'équipe SSI doit vérifier et contrôler les interconnexions de réseaux. Des serveurs proxy sont utilisés pour le filtrage des sites web. Le filtrage s'applique dans les deux sens.

Il convient que les liaisons de l'INSERM avec internet soient si possible redondées et protégées par des pare-feu.

| 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 l'INSERM doit être réalisé à l'aide de serveurs proxys et de firewalls. Un filtrage des connexions interne vers l'extérieur doit être réalisé à l'aide d'un pare-feu

Le réseau public de l'INSERM accessible par les usagers extérieurs ne doit pas contenir d'informations confidentielles.

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

Il convient que l'INSERM sensibilise le personnel sur l'importance du chiffrement des informations.

Il convient que l'INSERM formalise une procédure de chiffrement des informations 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 |
|---|---|---|

L'INSERM doit cloisonner son SI en sous réseaux.

L'INSERM met en place un vlan spécifique pour les activités d'administration.

### 3.6.3.Accès spécifiques

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

L'INSERM doit mettre en place des interconnexions de réseaux locaux contrôlées et sécurisées.

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

Les ressources informatiques de l'INSERM doivent être cloisonnées physiquement et logiquement.

| **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 RSSI à chaque type d'utilisation spécifique.

## 3.6.4.Usage sécurisé des réseaux sans fil

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

Le réseau sans fil est utilisable par le personnel de l'INSERM ainsi que par les visiteurs.

Le réseau sans fil de l'INSERM doit être sécurisé par un mot de passe. Ce dernier doit être séparé physiquement du réseau interne de l'INSERM.

Les accès aux réseaux internes depuis le réseau sans fil doivent passer par les mêmes contrôles que les accès depuis Internet, ou être cloisonnés dans un réseau logique dédié, aux ressources limitées.

## 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** |
|---|---|---|

Le filtrage MAC est le moyen minimal utilisé pour limiter les attaques sur les couches basses.

Il convient d'améliorer les mécanismes de protection des couches basses.

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

Le fournisseur d'infrastructure doit fournir les plages d'adresses IP pour le routage statique en interne.

Il convient de surveiller les annonces de routage dynamique.

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

Tous les mots de passes par défaut des équipements du SI de l'INSERM doivent être systématiquement changés et les certificats SSL de l'INSERM doivent être installés.

Un processus de renouvellement de certificats et une automatisation du processus doit être réalisée au sein de l'INSERM.

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

Au sein de l'INSERM les interfaces et services inutiles doivent être systématiquement désactiver afin de durcir la configuration des équipements réseaux.

Il convient d'établir un tableau de bord de la configuration de ces équipements.

## 3.6.6.Cartographie réseau

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

Une architecture réseau doit être formalisée et tenue à jour par l'INSERM.

Il convient de régulièrement mettre à jour la cartographie réseau pour répondre aux évolutions du réseau du SI.

Il convient d'intégrer la configuration des équipements aux schémas de l'architecture réseau et de mettre en place des mesures adéquates afin de protéger ces 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 |
|---|---|---|

L'INSERM doit mettre en œuvre des zones dématérialisées (DMZ) afin de cloisonner et protéger ses services accessibles depuis l'extérieur.

L'INSERM doit mettre en œuvre un ensemble de VLAN afin de segmenter son LAN en sous-réseaux isolés.

Au niveau des SI le principe de séparation des flux d'administration de ceux qui permettent d'accéder aux applications doit être respecté.

| Architecture de stockage et de sauvegarde | Identifiant: | ARCHI-STOCKCI |
|---|---|---|

L'INSERM doit disposer d'une d'architecture de stockage.

Il convient à L'INSERM de mettre en place un réseau de stockage et de sauvegarde des données.

| Passerelle Internet | Identifiant: | ARCHI-PASS |
|---|---|---|

L'INSERM doit mettre en place un mécanisme de filtrage à l'aide d'un serveur proxy et d'un pare-feu 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 leur confidentialité et intégrité.

## 3.8.2.Surveillance et configuration des ressources informatiques

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

L'INSERM doit posséder un dispositif ou une procédure de journalisation permettant de tracer l'ensemble des interventions de maintenance sur les ressources informatiques.

Il convient que ces traces soient conservées à des fins de preuve et restent accessibles au RSSI pendant au moins un an.

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

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

L'INSERM doit appliquer un durcissement des systèmes d'exploitation et des logiciels sur l'ensemble du 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 l'INSERM dans le cadre du maintien en condition de sécurité. Ces modalités doivent faire l'objet d'un suivi selon un processus bien précis et formalisés.

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

L'INSERM doit posséder un document recensant la configuration des équipements réseaux en place de manière à pouvoir la répliquer sur un nouvel équipement.

L'INSERM doit déterminer une configuration standard et doit la déployer sur tout nouveau poste de travail ou serveur.

L'INSERM doit documenter la configuration de toutes les ressources informatiques. Cette documentation est mise à jour à chaque changement notable.

Il convient que l'INSERM dispose également d'une procédure de sauvegarde et de restauration des configurations pour ses équipements.

## 3.8.3.Autorisations et contrôles d'accès

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

L'INSERM doit exiger l'authentification de tout utilisateur ayant accès aux ressources non publiques, comme les applications métiers.

Les utilisateurs de l'INSERM doivent posséder des comptes nominatifs pour l'accès aux ressources.

L'INSERM 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 à l'INSERM de définir le niveau de sensibilité, le besoin de diffusion et de partage des ressources.

Il convient que chaque utilisateur dispose de droits d'accès aux seules ressources dont il a besoin dans le cadre de son travail.

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

L'INSERM doit mettre en œuvre des mécanismes permettant de limiter les services, les données et les privilèges auxquels ont accès les utilisateurs en fonction de leurs rôles et responsabilités au sein de l'INSERM. Ces mécanismes reposent sur l'attribution d'identifiants et de mécanisme d'authentification aux différentes applications métiers.

Il convient à L'INSERM de définir et de mettre à jour la liste des profils utilisateurs ayant accès aux données sensibles.

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

L'INSERM doit formaliser un processus d'autorisation gérant les accès utilisateurs aux ressources du SI de l'INSERM.

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 |
|---|---|---|

Le RSSI de l'INSERM doit revoir périodiquement les autorisations d'accès à minima tous les ans.

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

Les informations d'authentification de l'INSERM doivent être considérées comme étant des données sensibles.

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

L'INSERM interdit aux utilisateurs le stockage des mots de passe en clair sur leurs postes de travail. Il est interdit également de les stockés sur supports papier (post-it).

L'INSERM doit utiliser des protocoles chiffrés permettant de ne pas diffuser en clair les mots de passe sur le réseau.

Les mots de passe des postes utilisateurs et administrateurs sont gérés via une politique de mots de passe.

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

Lors de la création d'un compte utilisateur au sein de l'INSERM un mot de passe aléatoire unique doit être généré.

Il convient que l'utilisateur soit amené à changer son mot de passe lors de la première utilisation.

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

L'INSERM doit mettre en œuvre des règles de gestion et de protection permettant d'imposer une politique de mots de passe.

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, basée a minima sur les recommandations en cours parues au Journal Officiel

| Utilisation de certificats électroniques | Identifiant: | EXP-CERTIFS |
|---|---|---|

Au sein 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)

Il convient si possible que l'INSERM dispose d'un contrôle interne en charge de la vérification de l'application de la politique de mot de passe en conformité avec la PSSI.

| **Séquestre des authentifiants « administrateur »** | **Identifiant:** | **EXP-SEQ-ADMIN** |
|---|---|---|

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

L'INSERM 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 de l'INSERM doit disposer d'un mot de passe spécifique et destiné exclusivement à l'administration SI.

Le mot de passe administrateur doit être distinct du mot de passe utilisateur

| **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 d'interdire par défaut les droits d'administrations sur les postes de travail des utilisateurs.

Les utilisateurs ayant des droits d'administration accordés par dérogation ne doivent les avoir que sur leur poste de travail personnellement attribué.

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

L'utilisation des outils et interfaces d'administration doit être strictement limitée aux administrateurs du SI de l'INSERM.

Il convient d'élaborer une procédure formelle d'autorisation d'accès aux outils d'administration.

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

Il convient d'élaborer une procédure formalisée définissant les droits d'accès administrateurs.

Cette procédure doit être connue et validée par une autorité au sein l'INSERM.

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

Les actions d'administrations sur le SI de l'INSERM doivent être tracées.

Il convient si possible que le mécanisme déployé à cet effet puisse permettre de gérer au niveau individuel l'imputabilité de ces actions d'administration.

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

L'INSERM doit utiliser des protocoles sécurisés (SSH, HTTPS) pour administrer ses ressources.

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

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

| **Centraliser la gestion du système d'information** | **Identifiant:** | **EXP-CENTRAL** |
|---|---|---|

Afin de gérer efficacement le parc informatique, l'administration des systèmes d'information doit être centralisée le plus possible via un bastion d'administration.

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

L'INSERM doit mettre en place un moyen de prise en main à distance sécurisé.

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

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

L'INSERM doit disposer d'une procédure de gestion des comptes.

Il convient de formaliser cette procédure et de la mettre à jour régulièrement.

| 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) au sein de l'INSERM.

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

Une limitation en nombre d'effectif doit être appliquée quant à l'appartenance aux groupes d'administrateurs du domaine.

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

L'INSERM 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 |
|---|---|---|

L'INSERM doit appliquer un contrôle d'accès à l'ensemble des comptes de services en respectant le principe du moindre privilège.

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

Il convient de supprimer systématiquement tous les comptes obsolètes ou inutilisés.

Il convient de supprimer ou de désactiver les comptes utilisateurs au plus tard six mois après leur départ.

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

Un mot de passe unique et distinct doit être utilisé pour chaque compte local d'administration sur chaque machine au sein de l'INSERM, afin d'empêcher la réutilisation des empreintes d'un compte utilisateur local d'une machine à une autre.

| **Maintenance externe** | **Identifiant:** | **EXP-MAINT-EXT** |
|---|---|---|

Il convient d'effacer les données non chiffrées de toute ressource informatique sensible 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** |
|---|---|---|

Il convient que les données présentes sur les disques durs ou la mémoire intégrée, de toute ressources informatiques (poste, support, serveurs, nomades, mobiles) étant amenée à quitter définitivement L'INSERM soient effacées de manière sécurisée.

Il convient d'utiliser des produits labélisés pour effacer les données sensibles et de formaliser cette procédure.

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

Tous les équipements vulnérables de 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 les évènements antivirus.

Il convient de pouvoir corréler les évènements anti-virus avec les autres évènements de sécurités.

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

Les mises à jour d'antivirus doivent être automatiquement et systématiquement déployées sur l'ensemble des équipements concernés.

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

Il convient de configurer de manière sécurisée le navigateur internet déployé sur les SI de l'INSERM (ex : désactivation 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** |
|---|---|---|

L'INSERM doit définir et mettre en place une politique de suivi et d'application des correctifs de sécurité sur le parc informatique de l'INSERM. Il convient que cette politique soit régulièrement améliorée.

Il convient que l'INSERM effectue un suivi des correctifs de sécurité appliqués.

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

Les correctifs de sécurités doivent être déployés régulièrement sur les SI de l'INSERM.

| **Assurer la migration des systèmes obsolètes** | **Identifiant:** | **EXP-OBSOLET** |
|---|---|---|

Il convient de s'assurer que les versions des logiciels utilisées soient à jour et que leur support soit maintenu par l'éditeur.

| **Isoler les systèmes obsolètes restants** | **Identifiant:** | **EXP-ISOL** |
|---|---|---|

Des systèmes obsolètes au sein des SI de l'INSERM peuvent être gardés volontairement pour assurer la continuité opérationnelle des projets.

Il convient de prendre des mesures adéquates vis-à-vis de ces systèmes pour les confiner.

| Journalisation des alertes | Identifiant: | EXP-JOUR-SUR |
|---|---|---|

L'INSERM doit mettre en place des dispositifs de journalisation pour chaque système.

Il convient de conserver les journaux d'évènements de manière sécurisée et de les centraliser si possible.

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

L'INSERM doit disposer d'une politique de gestion des journaux d'évènements de sécurité.

Il convient que l'INSERM dispose d'une politique pour l'analyse des journaux.

| Conservation des journaux | Identifiant: | EXP-CONS-JOUR |
|---|---|---|

L'INSERM doit conserver les journaux d'évènements pendant douze mois.

## 3.8.5.Défense des systèmes d'information

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

Les équipes en charge de la SSI de l'INSERM doivent analyser les journaux d'évènements en fonction des besoins et des incidents signalés.

L'analyse des flux réseaux entrants et sortants peut être effectuée sur demande par le fournisseur d'infrastructure.

| Maîtrise des matériels | Identifiant: | EXP-MAIT-MAT |
|---|---|---|

L'INSERM doit effectuer un filtrage par adresse MAC pour s'assurer de l'impossibilité de connecter des équipements non-autorisés au SI.

Il est interdit de connecter au SI des supports amovibles et des disques de stockage personnel.

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

Les postes fixes de l'INSERM doivent être installés dans des bureaux pouvant être fermés à clé.

Il convient que tous les postes fixes sensibles de l'INSERM soient protégés physiquement contre le vol par l'intermédiaire d'un câble anti-vol.

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

Il convient que les supports amovibles contenant des informations sensibles soient chiffrées.

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

Toute perte, vol ou intrusion sur une ressource du SI doit être systématiquement déclarée au RSSI et au FSD.

| **Réaffectation de matériels informatiques** | **Identifiant:** | **EXP-REAFFECT** |
|---|---|---|

Il convient de formaliser la procédure de gestion du matériel informatique 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 l'INSERM homologue à minima les équipements nomades ayant un niveau de sensibilité critique.

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

L'accès à distance au SI interne doit s'effectuer par l'utilisation d'un VPN sécurisé.

| **Impression des informations sensibles** | **Identifiant:** | **EXP-IMP-SENS** |
|---|---|---|

Une procédure d'impression sécurisée au sein de l'INSERM doit être utilisée quel que soit les données concernées.

L'INSERM doit disposer d'un mécanisme d'authentification sur les impressions, pour l'ensemble des utilisateurs des SI.

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

L'INSERM doit mettre en œuvre des mesures de sécurité pour protéger les imprimantes de l'extérieur.

# 3.8.6.Exploitation sécurisée des centres informatique

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

Tout système d'exploitation déployé au sein de l'INSERM doit faire l'objet d'un support valide de la part de son éditeur.

Seuls les services et les applications nécessaires doivent être installés, de façon à réduire la surface d'attaque.

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

La configuration des logiciels déployés en tiers présentation au sein l'INSERM doit être renforcée.

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

Les logiciels en tiers application doivent faire l'objet d'un développement sécurisé piloté ou validé par l'INSERM.

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

L'INSERM doit appliquer des règles très strictes aux logiciels en tiers données.

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

Les échanges de fichiers de l'INSERM doivent être effectués via des protocoles sécurisés.

| **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'INSERM.

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

Des mécanismes de filtrage et de cloisonnement des flux applicatifs doivent être mis en place pour protéger les SI de l'INSERM contre les attaques informatiques.

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

Les flux d'administrations systèmes doivent être séparés des flux d'administrations applicatifs. Ces flux sont protégés via un mécanisme de cloisonnement logique.

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

Dans le cadre d'éventuelle réutilisation des disques durs contenant des données sensibles, il convient que ceux-ci fassent l'objet d'un effacement sécurisé au préalable.

Il convient de formaliser les procédures d'effacements des disques dur pour permettre leur réutilisation et reconditionnement éventuel.

| **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** |
|---|---|---|

Afin d'assurer une cohérence dans les échanges entre applications et une traçabilité pertinente des évènements techniques, le service NTP doit être utilisé sur l'ensemble des équipements du SI de l'INSERM.

| **Supervision** | **Identifiant:** | **EXP-CI-SUPERVIS** |
|---|---|---|

Il convient que les flux de supervision et les flux d'administration au sein de l'INSERM soient cloisonnés.

| 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 |
|---|---|---|

Les opérations de gestion des accès aux réseaux (ex : contrôle physique des accès, attribution des adresses IP, filtrage des informations) de L'INSERM doivent être soumises à des procédures sécurisées.

| Audit/contrôle | Identifiant: | EXP-CI-AUDIT |
|---|---|---|

Il convient que L'INSERM effectue des audits sur son 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 aux équipes SI de l'INSERM de gérer l'ensemble des équipements du parc Inserm informatique fixe, mobile, et nomade. | | |

| **Formalisation de la configuration des postes des travail** | **Identifiant:** | **PDT-CONFIG** |
|---|---|---|
| Une procédure de durcissement de la configuration des postes de travail doit être appliquée.<br><br>Il convient que cette procédure soit vérifiée et formalisée par l'INSERM. | | |

| **Verrouillage de l'unité centrale des postes fixes** | **Identifiant:** | **PDT-VEROUIL-FIXE** |
|---|---|---|
| Il convient que l'ensemble des postes fixes sensibles soient protégé par des systèmes antivols. | | |

| **Verrouillage des postes portables** | **Identifiant:** | **PDT-VEROUIL-PORT** |
|---|---|---|
| Il convient que l'ensemble des postes portables soit protégé par des systèmes antivols.<br><br>Il convient que l'ensemble des téléphones portables soit protégé par des systèmes de verrouillage à distance<br><br>Il convient de sensibiliser les utilisateurs à leur utilisation. | | |

| **Réaffectation du poste de travail** | **Identifiant:** | **PDT-REAFFECT** |
|---|---|---|
| Il convient de mettre en place une procédure de sécurité décrivant les règles concernant la réaffectation des postes. | | |

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

Le principe du moindre privilège doit être appliqué aux droits utilisateurs sur tous les postes de travail. Les utilisateurs ne doivent pas être administrateurs sur leurs postes de travail, sauf dérogation.

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

Les privilèges d'accès "administrateur" doivent être utilisés uniquement pour les actions d'administration et sont distincts des comptes utilisateurs.

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

L'accès aux comptes administrateurs des postes doit être limité aux équipes SI de l'INSERM.

Les mots de passes par défaut des comptes administrateurs locaux doivent être systématiquement supprimés.

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

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

Les données de l'espace réseau de l'INSERM doivent être sauvegardées.

Il convient que la sauvegarde soit effectuée à intervalle régulier.

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

L'INSERM doit disposer de moyens de synchronisation ou de sauvegarde des données locales pour les utilisateurs.

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

Afin de limiter la surface d'attaques et de divulgation des données en interne, L'INSERM doit interdire systématiquement le partage de répertoires ou de fichiers hébergés localement sur les postes de travail.

Il convient d'utiliser exclusivement les serveurs de fichiers mis à disposition.

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

Il convient de supprimer les données présentes sur les postes dédiés à la formation ou aux présentations entre deux utilisations.

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

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

Il convient de chiffrer l'ensemble des données sensibles sur les serveurs utilisés au sein de l'INSERM. Il convient 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 est interdit de connecter des terminaux amovibles personnels sur les postes de travail.

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

Afin de maîtriser la sécurité des accès à distance au SI de l'INSERM, ceux-ci doivent être réalisés via son infrastructure.

| **Pare-feu local** | **Identifiant:** | **PDT-NOMAD-PAREFEU** |
|---|---|---|

Il convient si possible d'installer un pare-feu local sur les équipements nomades du SI de l'INSERM.

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

Le stockage d'information sur les postes nomades doit être limité au strict nécessaire.

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

| **Filtre de confidentialité** | **Identifiant:** | **PDT-NOMAD-FILT** |
|---|---|---|

Des filtres de confidentialité doivent être fournis sur demande et à utiliser systématiquement dès que ces postes sont hors du périmètre de l'INSERM.

Il convient de fournir par défaut des filtres de confidentialité sur l'ensemble des 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.

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 de désactiver les interfaces sans fil (ex : Wifi, Bluetooth, 3G…) non utilisées sur les postes de travail de 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** |
|---|---|---|

Tous les mots de passe par défaut des équipements doivent être changés dès leur mises en fonctions.

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 de l'INSERM doit être limité à une seule adresse de messagerie à la fois.

## 3.9.3.Sécurisation de la téléphonie

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

La téléphonie sur IP (TOIP) doit être privilégiée.

L'INSERM doit effectuer un durcissement des autocommutateurs analogiques dans le cas contraire.

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

Il convient que les messageries vocales de l'INSERM soient toutes protégées par un mot de passe à code pin différent du code par défaut.

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

L'utilisation du DECT (téléphone sans fil) doit être restreinte.

Il convient de formaliser une dérogation pour l'utilisation des DECT au sein de l'INSERM.

| Attribution des accès téléphoniques | Identifiant: | PDT-TEL-INSERM |
|---|---|---|

Il convient que les équipements téléphoniques soient alloués à une salle ou une personne en particulier.

## 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.

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

Il convient 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 des mesures de sécurité à partir de l'étape de conception jusqu'à l'étape de retrait (ex : 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, privacy by design …). | | |

| **Intégrer des clauses SSI dans les contrats de sous-traitance de développement informatique** | **Identifiant:** | **DEV-SOUS-TRAIT** |
|---|---|---|
| Des exigences de sécurités doivent être formalisés (ex : TOP 10 OWASP). Les partenaires doivent s'engager par le plan d'assurance sécurité (PAS) à respecter les normes de développement sécurisé. | | |

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.

| **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.

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

Il convient d'inclure dans le cahier des clauses techniques particulières (CCTP) des critères de sécurisation pour les phases d'intégration avec les prestataires développeurs.

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

L'INSERM doit disposer des règles de sécurités 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 l'INSERM doivent respecter à minima le top 10 OWASP (Open Web Application Security Project) afin de prendre en compte la sécurité dans les développements web.

Des prérequis sécurité supplémentaires peuvent être exigés.

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

Il convient d'utiliser différentes technologies de cryptologie afin de protéger les mots de passes stockés.

L'INSERM doit 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** |
|---|---|---|

L'INSERM doit 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.

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** |
|---|---|---|

L'INSERM doit formaliser 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. L'organisation doit 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 couvrant les applications nationales.

La chaîne fonctionnelle SSI doit contribuer à la qualification de l'incident, à son pilotage et à son traitement. Le RSSI est le chef de projet qui qualifie et pilote le traitement des risques.

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

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 ministériel de continuité d'activité des Systèmes d'Information** | **Identifiant:** | **PCA-MINIS** |
|---|---|---|

Il convient de réaliser un plan de continuité d'activité (PCA) de l'établissement.

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

Il convient que l'INSERM réalise et formalise un plan de continuité d'activité SI (PCI) ;

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 le RSSI soit garant de la mise en œuvre du PCI, de son test, de son maintien à jour et de son application en cas de besoin.

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

L'INSERM doit instaurer des moyens techniques de redondance au niveau de certains équipements.

Il convient que ces moyens techniques soit généralisé dans la mesure du possible.

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'INSERM formalise ces dispositifs techniques dans le plan de continuité d'activité SI et rédige des procédures opérationnelles facilitant leurs mises en œuvre.

| **Protection de la disponibilité des sauvegardes** | **Identifiant:** | **PCA-SAUVE** |
|---|---|---|

Il convient que Les données sauvegardées soient répliquées sur plusieurs sites géographiquement distants en adéquation avec les besoins de disponibilité du PCI.

| **Protection de la confidentialité des sauvegardes** | **Identifiant:** | **PCA-PROT** |
|---|---|---|

Il convient que l'INSERM met en œuvre un contrôle d'accès aux données sauvegardées.

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 de manière régulière. 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, …).

# 3.13. Conformité, audit, inspection, contrôle

## 3.13.1. Contrôles réguliers

| Contrôles locaux | Identifiant: | CONTR-SSI |
|---|---|---|

Il convient à 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 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 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 |
|---|---|---|

Un bilan annuel mesurant la maturité du SSI globale doit être fourni à l'ANSSI 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 :

Les régles suivantes de la PSSIE n'ont pas été retenues pour la PSSI administrative. Les motifs de la non sélection des ces régles sont explicités dans le corps des différentes régles.

| **Protection des informations sensibles au sein des zones d'accueil** | **Identifiant:** | **PHY-SENS** |
|---|---|---|
| L'INSERM ne dispose pas de zones ouvertes au public. | | |

| **Sécurisation du SI de sûreté** | **Identifiant:** | **PHY-SI-SUR** |
|---|---|---|
| L'INSERM ne dispose pas d'un SI de sûreté propre. | | |

| **Accès réseau en zone d'accueil du public** | **Identifiant:** | **PHY-PUBL** |
|---|---|---|
| L'INSERM ne dispose pas de lieu ouvert au public. | | |

| **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 de l'INSERM | | |

| **Sécuriser les sessions EGP** | **Identifiant:** | **RES-ROUTDYN-EGP** |
|---|---|---|
| Il n'y a pas de protocole de routage dynamique en place au sein de l'INSERM | | |

Inserm

La science pour la santé
From science to health