

## **Politique Générale de Sécurité du Système d'Information de l'AP-HP**

Juin 2017

Version 2.1 – Diffusion : Diffusion publique

## FICHE DE CONTROLE DU DOCUMENT

### Caractéristiques du document

Référence	PGSSI AP-HP
Identification :	Politique Générale de Sécurité du Système d'Information de l'AP-HP;
Objet :	<p>La Politique Générale de Sécurité du Système d'Information (PGSSI) a pour objectif de fournir un cadre de référence et de cohérence à la Sécurité du Système d'Information (SI) de l'AP-HP.</p> <p>Elle définit les principes généraux de sécurité à respecter au sein de l'AP-HP, ainsi que l'organisation et les responsabilités en matière de Sécurité du SI.</p>
Rédacteur	Membres du groupe de travail « Refonte PGSSI »
État	Validée
Version :	V2.0
Classification	Public

### Suivi des versions

Version	Date	Rédacteur	Modification
1.0	Mai 2010	Cellule de pilotage stratégique du système d'information	1 <sup>ère</sup> publication
2.0	Mai 2016	Direction des systèmes d'information / Sécurité des Systèmes d'information (DSI/SSI) et membre du groupe de travail « Refonte PGSSI »	Mise à jour par rapport aux évolutions de contexte Ajout des principes de sécurité liés à la responsabilisation des utilisateurs et des tiers
2.1	Juin 2017	SG/DSI/RSSI	Nomination d'un CIL Nouvelle organisation de la DSI Observations divers

## TABLE DES MATIERES

<i>Fiche de contrôle du document</i> .....	2
<i>Table des matières</i> .....	3
<b>1 Introduction</b> .....	4
1.1 Contexte.....	4
1.2 Périmètre d'application .....	4
1.3 Cadre de référence .....	4
1.4 Évolution de la PGSSI.....	5
<b>2 Enjeux et objectifs de l'AP-HP dans le domaine de la sécurité de l'information</b> ....	6
2.1 Répondre aux besoins de sécurité des métiers.....	6
2.2 S'aligner aux enjeux stratégiques du SI de l'AP-HP .....	6
2.3 Respecter les obligations légales.....	7
<b>3 Principes de mise en œuvre de la sécurité de l'information</b> .....	8
3.1 Pilotage de la sécurité par les risques .....	8
3.2 Responsabilisation des utilisateurs du SI et des tiers .....	12
3.3 Continuité du SI de l'AP-HP.....	13
3.4 Gestion et protection des accès aux biens et aux données .....	14
3.5 Protection des infrastructures .....	16
<b>4 Organisation et instances de pilotage</b> .....	17
4.1 Rôles et responsabilités.....	17
4.2 Instances de pilotage .....	22
<b>5 Glossaire</b> .....	25

## 1 INTRODUCTION

### 1.1 Contexte

La **Politique Générale de Sécurité du Système d'Information** (PGSSI) a pour objectif de fournir un cadre de référence et de cohérence à la Sécurité du Système d'Information (SI) de l'AP-HP.

Elle définit les principes généraux de sécurité à respecter au sein de l'AP-HP, ainsi que l'organisation et les responsabilités en matière de Sécurité du SI.

### 1.2 Périmètre d'application

La Politique Générale de Sécurité du SI s'applique à l'ensemble de l'AP-HP : la Direction Générale, les Directions Fonctionnelles, les Groupes Hospitaliers (GH), les hôpitaux hors groupes (Site), les Pôles d'Intérêt Commun (PIC) et la Direction des Systèmes d'Information (DSI).

La PGSSI s'applique aussi aux entités sous-traitantes et aux partenaires externes accédant au SI de l'AP-HP. Les entités chargées des relations contractuelles et opérationnelles avec ces sous-traitants ou partenaires doivent donc s'assurer du respect de la PGSSI sur le périmètre d'actions impactant le SI de l'AP-HP. En particulier, la Direction Spécialisée des finances publiques pour l'AP-HP, en tant que partenaire, doit s'assurer du respect de la PGSSI sur le périmètre du SI commun avec l'AP-HP.

Le SI est considéré dans son ensemble, c'est-à-dire comme la totalité des moyens organisationnels, matériels (serveurs, postes de travail, dont l'informatique biomédical, la gestion technique des bâtiments, réseaux, téléphonie, supports papier, ...) et logiciels de l'AP-HP visant à créer, acquérir, traiter, stocker, archiver, diffuser ou détruire de l'information.

Par ailleurs, la PGSSI s'applique aux usages impliquant une interaction avec le SI de l'AP-HP (connexion de postes de travail personnels, de recherche, ou échanges avec les réseaux de recherche, d'associations, ou de partenaires plus généralement).

La Politique Générale de Sécurité du SI couvre le SI de l'AP-HP, et non la sécurité dans son ensemble, c'est-à-dire la sécurité des personnes ou des moyens autres qu'informatiques (hygiène, sûreté des locaux et des outils de travail, respect de la législation du travail, ...).

En cas de non applicabilité d'un des principes de la présente Politique, une procédure de dérogation doit être engagée et instruite par le Responsable de la Sécurité des Systèmes d'Information de l'AP-HP.

### 1.3 Cadre de référence

La Sécurité du SI de l'AP-HP est formalisée dans un référentiel documentaire dont la présente **Politique Générale de Sécurité du SI** constitue le premier niveau, fixant les principes de sécurité et les orientations d'organisation.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Le cas échéant, elle peut exceptionnellement être déclinée au sein des directions fonctionnelles ou des GH/Site/PIC pour une adaptation aux besoins spécifiques sans remise en cause des principes édictés dans la présente Politique (Convention de sécurité entre des entités internes et/ou externes par exemple). Les documents traitant de la sécurité du SI et existant préalablement à cette PGSSI doivent également être en conformité avec les principes édictés. Dans le cas contraire, le Responsable Sécurité du Système d'Information (RSSI) du périmètre concerné (cf. le paragraphe 4.1.3. La filière Sécurité du Système d'Information de l'AP-HP) initiera une démarche d'adaptation.

De telles déclinaisons sont présentées à la filière sécurité pour avis, et validées par le Responsable Sécurité du Système d'Information (RSSI) de l'AP-HP.

En outre, le cadre de référence peut aussi être complété par des **Directives thématiques de Sécurité du SI** décrivant les règles opérationnelles à mettre en œuvre (sur la Gestion des Identités et des Accès ou le Plan de continuité informatique par exemple) et des guides méthodologiques.

Elle est complétée par une Charte d'Utilisation du SI de l'AP-HP décrivant les règles d'usage du SI annexée au règlement intérieur.

## 1.4 Évolution de la PGSSI

La PGSSI est un document pérenne, qui n'a pas vocation à évoluer régulièrement. Cependant, elle doit tenir compte des changements qui peuvent affecter les SI et leurs environnements, notamment en termes d'enjeux et de menaces.

La PGSSI doit en conséquence être mise à jour au regard des évolutions telles que :

- Les réorganisations (mise en place d'une nouvelle structure impactant le SI par exemple),
- Les évolutions significatives du SI et de ses conditions d'exploitation,
- Les changements majeurs de la législation et de la réglementation, ou des nouvelles normes nationales, européennes ou internationales,

L'évolution de la PGSSI est placée sous l'autorité du RSSI de l'AP-HP, qui déclenche les opérations nécessaires à sa mise à jour, propose, en s'appuyant sur la filière Sécurité du SI de l'AP-HP (Cf. le paragraphe 4.1.3 La filière Sécurité du Système d'Information de l'AP-HP), les révisions et les versions successives qu'il soumet aux instances de pilotage appropriées pour validation.

## 2 ENJEUX ET OBJECTIFS DE L'AP-HP DANS LE DOMAINE DE LA SECURITE DE L'INFORMATION

### 2.1 Répondre aux besoins de sécurité des métiers

Le respect des besoins de sécurité métiers de l'AP-HP est capital, tant pour les informations médicales, que pour les informations de gestion financières ou les données personnelles des agents par exemple. Ces besoins sont exprimés selon les quatre critères de sécurité que sont :

La **disponibilité** :

Le SI de l'AP-HP doit remplir ses fonctions dans des conditions prédéfinies d'horaire et de délai.

L'**intégrité** :

Le SI de l'AP-HP doit garantir l'exhaustivité, la validité et la cohérence des informations.

La **confidentialité** :

Le SI de l'AP-HP doit garantir que les informations ne sont accessibles que par des personnes habilitées et qu'elles ne peuvent pas être divulguées en dehors des règles établies.

La **traçabilité** :

Le SI de l'AP-HP doit assurer que les événements et les accès liés aux informations qui le nécessitent sont enregistrés à travers des traces accessibles et si besoin, opposables.

### 2.2 S'aligner aux enjeux stratégiques du SI de l'AP-HP

Le Sécurité du SI doit être en phase avec les objectifs stratégiques fixés pour le SI de l'AP-HP dans le cadre du plan stratégique 2015-2019 et du schéma directeur des systèmes d'information de l'AP-HP pour la période 2016-2020.

La PGSSI prend en compte les perspectives identifiées dans le plan stratégique, qui elles-mêmes se déclinent dans le schéma directeur des systèmes d'information, notamment dans le cadre des thématiques suivantes :

- Penser le parcours du patient de demain ;
- Faire de l'AP-HP un acteur des révolutions médicales et numériques ;
- Coopérer avec la médecine de premier recours ;
- Soutenir l'innovation ;
- Accélérer la transformation de nos organisations ;
- Faire évoluer la prise en charge pour mieux soigner.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Au-delà de l'enjeu direct lié à la prise en charge des patients et de la protection des informations nominatives, la PGSSI s'inscrit dans les démarches de certification des comptes et de la Haute autorité de santé – pour lesquelles il est demandé aux établissements de santé de justifier d'une politique de sécurité construite, documentée, connue de tous et maîtrisée sur le plan organisationnel.

## 2.3 Respecter les obligations légales

La mise en œuvre et l'utilisation du SI sont soumises à un ensemble de textes législatifs et réglementaires qui doit être respecté. En cas de manquement, de façon involontaire ou délibérée, la responsabilité de l'AP-HP peut être engagée sur le plan judiciaire, ainsi que celle des collaborateurs, sur le plan disciplinaire et/ou civil.

Il s'agit donc d'**assurer la conformité du SI de l'AP-HP aux exigences légales et réglementaires**, en particulier :

- la Loi Informatique et Libertés (LIL),
- le Code Pénal,
- le Code de la Santé Publique,
- le Code de la Propriété Intellectuelle,
- La certification HAS des groupes hospitaliers et des hôpitaux hors groupe,
- La certification des comptes,
- L'accréditation du COFRAC pour les laboratoires d'Analyses Biologiques Médicales,
- Le cadre réglementaire relatif à la sécurité de l'information imposé par l'État et l'administration : le Référentiel Général de Sécurité (RGS), la Loi de Programmation Militaire (LPM),
- Les politiques de sécurité des SI émises par l'État (PSSI-E), le Ministère de la Santé/Social (PSSI-S) et l'ASIP Santé.

Pour ce faire, le RSSI doit :

- Assurer une veille sur l'évolution du cadre réglementaire relatif aux SI du domaine de la Santé,
- Identifier les évolutions ayant un impact sur le SI de l'AP-HP.

## 3 PRINCIPES DE MISE EN ŒUVRE DE LA SECURITE DE L'INFORMATION

Les principes de sécurité détaillés dans le présent chapitre de la PGSSI s'articulent autour des thématiques suivantes :

- Pilotage de la sécurité par les risques ;
- Responsabilisation à la sécurité de l'information des collaborateurs et des tiers ;
- Continuité du SI de l'AP-HP ;
- Gestion et protection des accès aux données ;
- Protection des infrastructures.

### 3.1 Pilotage de la sécurité par les risques

#### 3.1.1 Inscrire la sécurité dans un cycle d'amélioration continue

La Sécurité de l'AP-HP s'inscrit dans une démarche d'amélioration continue, inspirée de la **norme internationale de gestion de la sécurité de l'information : ISO/IEC 27001**.

Le cycle passe par les étapes décrites ci-après :

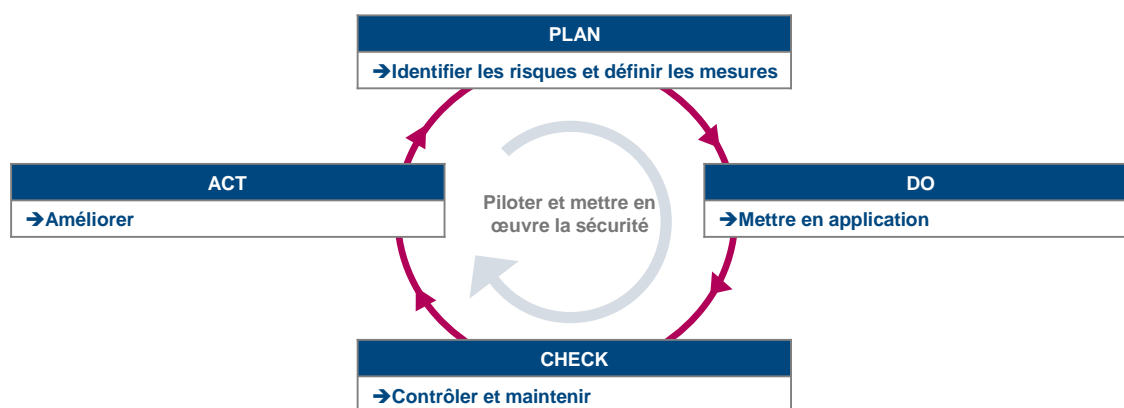


Figure 1 : Cycle de vie du pilotage et de la mise en œuvre des actions de sécurité

L'objectif d'une telle démarche est d'apporter des résultats concrets, mesurables et proportionnés aux risques. Ainsi, dans un premier temps, les risques sont appréciés et les mesures définies en conséquence (Plan), puis elles sont mises en œuvre (Do), et contrôlées (Check). Enfin, des actions correctives sont mises en place en fonction des écarts observés (Act).



# Politique Générale de Sécurité du Système d'Information de l'AP-HP

## 3.1.2 Identifier les risques et définir les mesures prioritaires

Les mesures de sécurité, quel qu'en soit le périmètre, doivent être définies au regard des risques.

Ce pilotage par les risques permet d'envisager les moyens organisationnels et techniques à mettre en place pour un juste niveau de sécurité au regard des enjeux.

Cette démarche doit s'intégrer au dispositif de gestion de risques existant à l'AP-HP, qui doit être décliné en matière de risques sécurité de l'information.

Ainsi, une analyse de risques sécurité des SI doit être déclinée à chaque niveau de l'AP-HP, conduite et revue régulièrement, en fonction des étapes suivantes :

- Identification des biens critiques et appréciation de leur criticité suivant les quatre critères de sécurité (disponibilité, intégrité, confidentialité, et traçabilité) ;
- Identification et appréciation des risques majeurs en fonction de l'état actuel du SI et des menaces ;
- Identification et mise en œuvre des mesures de sécurité appropriées sur les biens critiques, consignées dans des plans d'actions de traitement de risques.
- Suivi de plans de traitement et évaluation des risques résiduels par les responsables sécurité du SI et validation par les instances adéquates, en particulier les directions de chaque périmètre et le comité de pilotage sécurité.

## 3.1.3 Intégrer la sécurité dans les projets ayant une composante SI

Les projets comportant une composante SI (nouvelles applications, nouveaux systèmes ou équipements, mais aussi maintenance évolutive, évolutions d'infrastructure) doivent intégrer la démarche sécurité.

Les commanditaires du projet (les métiers accompagnés de leur maîtrise d'ouvrage) doivent exprimer les besoins de sécurité dès la phase de lancement du projet et doivent s'assurer de la mise à disposition des moyens pour y répondre.

Les chefs de projet maîtrise d'ouvrage et maîtrise d'œuvre doivent garantir l'intégration de la sécurité à chaque étape du projet. L'ensemble des étapes doivent être menées en concertation avec le RSSI de leur périmètre.

Les principales étapes attendues sont les suivantes :

- Identifier les biens critiques en fonction des enjeux exprimés par la direction métier commanditaire.
- Conduire l'analyse des risques et des contraintes, et identifier en conséquence les besoins et niveaux de sécurité à atteindre.
- Définir, proposer et mettre en œuvre les moyens et les actions de sécurité en réponse aux besoins exprimés.
- Assurer un suivi de la mise en œuvre des moyens de sécurité.
- Valider l'adéquation de la solution livrée par rapport aux objectifs de sécurité (par une phase de recette).
- Déclencher, si besoin, des actions correctrices pour atteindre ces objectifs.

## Politique Générale de Sécurité du Système d'Information de l'AP-HP

- Dans le cadre de prestation avec les tiers, spécifier de façon formelle, leur responsabilité et leur implication vis-à-vis du SI. En particulier, le chef de projet doit veiller à ce que des clauses de sécurité soient intégrées aux contrats de prestation qu'ils souscriraient avec des tiers. A minima, les exigences de confidentialité seront précisées.
- Faire valider les risques résiduels par les commanditaires du projet avant la mise en production du SI.

Les projets entrant dans le champ obligatoire du référentiel général (RGS) de sécurité, les téléservices de l'administration électronique et les interconnexions de SI entre autorités administratives, font l'objet d'une homologation de sécurité.

Par ailleurs, les Chefs de Projet veillent à la séparation et à la sécurisation des environnements de développement, de qualification/recette, de pré-production et de production.

Enfin, l'utilisation des données de production pour tester et qualifier une application ou une infrastructure, ne peut pas être effectuée sans l'accord du responsable de traitement concerné(s).

### 3.1.4 Assurer la conformité à la Loi Informatique et Libertés

La constitution de fichiers informatiques comportant des données à caractère personnel, c'est-à-dire permettant d'identifier directement ou indirectement une personne physique, est encadrée par des règles strictes édictées par la Commission Nationale de l'Informatique et des Libertés (CNIL).

La création d'un traitement automatisé de données à caractère personnel suppose ainsi, préalablement à sa mise en œuvre, l'accomplissement d'une formalité déclarative.

Le Correspondant Informatique et Libertés (CIL) est chargé de la gestion des traitements centraux de données à caractère personnel qui sont sous la responsabilité d'une direction fonctionnelle ou d'un PIC du Siège.

Toute personne ou service, souhaitant mettre en place un traitement de données à caractère personnel local doit se rapprocher, au préalable, du référent Loi Informatique et Libertés (LIL) dont il relève.

### 3.1.5 Suivre l'efficacité des mesures de sécurité

Des contrôles doivent être mis en place afin de mesurer l'efficacité du dispositif de sécurité et d'assurer le suivi des actions de sécurité en termes d'avancement et d'efficacité sur le traitement des risques.

Ces contrôles peuvent être permanents (par le suivi d'indicateurs, contrôle interne), ou ponctuels par la conduite d'audits techniques ou organisationnels.

Certains des contrôles peuvent donc s'inscrire dans le dispositif de contrôle interne afin d'intégrer le processus à l'organisation de l'AP-HP en systématisant la démarche. Toutefois, la réalisation de contrôles externes est indispensable puisqu'ils permettent de porter un nouveau regard sur le niveau de sécurité du SI de l'AP-HP.

### 3.1.6 Se conformer à la PGSSI

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Les cas de non-conformité à la présente PGSSI quelle qu'en soit leur cause (impossibilité technique, législation locale, ou arbitrage économique par exemple), doivent être **signalés au RSSI de l'AP-HP**, avec indication des éventuelles mesures prises pour limiter les conséquences de ces situations ou éviter qu'elles ne se reproduisent. Le RSSI de l'AP-HP accordera alors une dérogation tracée, limitée dans le temps, et réévaluée régulièrement.

Le cas échéant, le RSSI AP-HP pourra en référer au comité sécurité approprié, pour validation.

## 3.1.7 Gérer les incidents de sécurité et les crises

La survenue d'un incident de sécurité doit être signalée par tout utilisateur du SI (internes ou externes). Il s'agit notamment des incidents correspondant aux typologies suivantes telle que recommandée par le Ministère des affaires sociales (MAS) :

- Accès, modification, collecte non autorisés de données,
- Divulgence d'information,
- Intrusion / prise de contrôle (atteinte à la messagerie, attaques de site Web, intrusion logique via le réseau, interception de communication)
- Comportements anormaux : usages frauduleux, usages abusifs (abus de droit d'un utilisateur ou d'un administrateur), comportements déviants...
- Présence de fichiers malveillants (malwares),
- Dysfonctionnement d'ampleur (dénier de service, indisponibilité de service non expliquée...),
- Vulnérabilités critiques (vulnérabilités logicielles, vulnérabilités de configurations...).

Des moyens doivent être mis en œuvre pour permettre d'identifier les incidents de sécurité et de mesurer leurs impacts, quelles qu'en soient leurs origines (accidentelle, négligence, ou malveillance).

L'objectif est de :

- Pouvoir les partager entre acteurs de la filière sécurité et avec les entités concernées,
- Pouvoir les contrôler,
- Rétablir au plus vite le fonctionnement nominal,
- Éviter leur reproduction.

L'organisation et les procédures de gestion des incidents de sécurité doivent s'inscrire dans un cadre plus général de gestion des incidents SI de l'AP-HP.

Les incidents graves de sécurité des systèmes d'information, qui seraient générateurs d'une situation exceptionnelle au sein de l'AP-HP sont traités conformément au décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information.

Par ailleurs, un plan de gestion de crise sécurité majeure et transverse sur le SI de l'AP-HP doit être défini et formalisé afin de gérer les incidents de sécurité majeurs.

Ce plan doit spécifier les moyens humains, techniques et organisationnels à mettre en œuvre en fonction du type d'incident de sécurité (sinistre, piratage informatique...) et au regard des interdépendances entre les processus métiers.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Chaque entité SI doit mettre en place son organisation de crise afin de traiter les cas d'incidents de sécurité majeurs non transverses.

Les contrats concernant des prestations externes, en particulier d'assistance technique, de tierce maintenance applicative et de sous-traitance doivent comporter des clauses contractuelles spécifiques sur les modalités de remontée et de partage des incidents de sécurité survenus et pour délimiter la responsabilité des contractants en cas de survenu d'un incident de sécurité ou de situation de crise.

## 3.2 Responsabilisation des utilisateurs du SI et des tiers

### 3.2.1 S'assurer de la diffusion des comportements adaptés et des bonnes pratiques auprès des utilisateurs

Afin de permettre un fonctionnement optimal des systèmes d'information, des moyens doivent être mis en œuvre afin de favoriser la prise de conscience des enjeux liés à la sécurité des SI et la bonne application des règles de sécurité par les utilisateurs du SI.

Une charte de bon usage des systèmes d'information est formalisée et annexé au règlement intérieur. Elle réglemente les pratiques en termes d'utilisation des composants du SI de l'AP-HP et traite notamment des sujets suivants :

- Les règles relatives à la sécurité des équipements mis à disposition des utilisateurs,
- Les règles relatives à la connexion au SI d'équipements non fournis par l'AP-HP,
- Les règles relatives au droit d'accès et mots de passe,
- Les règles relatives à l'utilisation d'Internet et de la messagerie électronique,
- La remontée des incidents de sécurité par les utilisateurs,
- Les mesures de traçabilité et les procédures de contrôle mises en œuvre, ainsi que les sanctions applicables.

Un plan de sensibilisation doit être défini et mis en œuvre selon les besoins métiers, en collaboration avec les Directions Fonctionnelles et le RSSI concerné, afin de sensibiliser tous les catégories d'utilisateurs du SI de l'AP-HP (utilisateurs/personnel sans privilège, administrateurs et exploitants informatiques, personnel biomédical, maîtrise d'ouvrage etc.) au respect des règles de sécurité édictées et prévenir des erreurs humaines en matière de sécurité des SI.

Par ailleurs, un plan de formation adapté des acteurs de la sécurité (RSSI, équipe en charge de la sécurité opérationnelle) et des populations sensibles (administrateurs) doit être défini afin de leur permettre d'acquérir ou de renforcer les compétences nécessaires au bon exercice de leur fonction.

### 3.2.2 S'assurer de la prise en compte de la sécurité par les tiers

Des moyens doivent être mis en œuvre afin de s'assurer de la prise en compte de la sécurité dans les missions confiées à des tiers (fournisseurs, prestataires, partenaires) :

- Toute demande d'accès au SI de l'AP-HP confiée à un tiers fait l'objet d'une justification du bien-fondé de la demande auprès du RSSI du périmètre concerné.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Suite à validation de la demande, des mesures appropriées sont mises en place afin de permettre un accès au SI et la réalisation des missions confiées au tiers en conformité avec la PGSSI et aux exigences réglementaires applicables.

En particulier, l'accès à distance au SI de l'AP-HP et les opérations de télémaintenance doivent être sécurisés.

- Lors de la conduite d'appel d'offre, les exigences de sécurité attendues de la mission confiée au tiers sont clairement exprimées dans le dossier de consultation.
- Lors de la contractualisation, le tiers doit être responsabilisé vis-à-vis de la sécurité du SI : des clauses de sécurité doivent être intégrées aux contrats ; *a minima*, les exigences de confidentialité doivent être précisées.
- Tout au long de la relation avec le tiers, le respect des exigences de sécurité par le tiers doit être contrôlé par le responsable du contrat.

## 3.3 Continuité du SI de l'AP-HP

### 3.3.1 Mettre en place une continuité d'activités SI

Dans la mesure où le SI est support d'activités critiques de l'AP-HP, cette dernière doit mettre en place un Plan de Continuité des Activités (PCA) de son SI. Ce plan repose sur les deux volets suivants :

- La continuité des Métiers du SI au travers d'une procédure de gestion de crise et de modes dégradés (en permettant aux acteurs SI de continuer leur activité en cas de sinistre sur leurs locaux de travail par exemple),
- La continuité ou le secours informatique (moyens informatiques et de télécommunication).

Dans le cadre plus général de la continuité d'activités de l'AP-HP, la fonction SI doit apporter le support nécessaire à la mise en place des Plans de Continuité d'Activités Métiers.

La stratégie de continuité du SI est déterminée et mise en œuvre selon la criticité des activités SI déterminée par une analyse d'impact sur les activités et les scénarios de risques à couvrir.

Cette criticité est évaluée en fonction des niveaux d'impact (pertes financières, atteintes à l'image, conséquences sociales ou juridiques par exemple) d'une indisponibilité partielle ou totale des acteurs SI pour la continuité des Métiers SI, et des moyens informatiques et de télécommunication pour la continuité informatique.

### 3.3.2 Définir et mettre en œuvre un Plan de Secours Informatique (PSI)

L'AP-HP est dotée d'un Plan de Secours Informatique (PSI) de façon à ce qu'en cas de sinistre sur le SI, la continuité des activités critiques soit assurée.

Les niveaux de criticité des moyens informatiques se traduisent par un besoin de continuité exprimé en :

- Le Délai d'Interruption Maximal Admissible (DIMA),
- La Perte de Données Maximale Admissible (PDMA).

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Le plan de secours informatique précise :

- Les types de sinistres couverts (perte d'équipement, perte de salle informatique, ...),
- Le périmètre secouru,
- Les principes de secours des serveurs (serveurs dédiés, serveurs mutualisés...), des données (sauvegardes, externalisation de bandes ou réplication), du réseau et des postes de travail. A minima, les données doivent être sauvegardées, et les plus critiques, externalisées ou répliquées.

Si besoin, les modes dégradés permettant un fonctionnement sans informatique, doivent être identifiés et partagés entre les acteurs de la sécurité de l'AP-HP. Les utilisateurs doivent être informés de ces modes de fonctionnement.

Pour les prestations délivrées par un tiers (opérateurs télécoms, fournisseur d'accès Internet...), les engagements de niveau de disponibilité sont explicitement formalisés dans les contrats et les moyens prévus pour pallier l'indisponibilité éventuelle des ressources (personnels, données, procédures, matériel, ou logiciel) doivent être fournis par les prestataires.

Le Plan de Secours Informatique (PSI) s'articule avec la stratégie de continuité d'activités de l'AP-HP.

## 3.3.3 Maintenir le Plan de Continuité des Activités SI

Le Plan de Continuité des Activités SI de l'AP-HP doit être maintenu dans le temps par :

- La mise en place de processus de mises à jour passant notamment par la revue du périmètre, l'actualisation des documents, et les audits,
- Des tests et exercices réguliers du périmètre secouru.

## 3.3.4 Gérer les changements et les évolutions sans dégrader le niveau de service

Les impacts dus à des changements doivent être étudiés afin de ne pas porter atteinte à la disponibilité du SI.

Les propriétaires des processus concernés doivent être préalablement informés et doivent valider les évolutions au regard des impacts.

Le Plan de Continuité des Activités SI doit être maintenu à jour en fonction des changements organisationnels ou techniques.

## 3.4 Gestion et protection des accès aux biens et aux données

### 3.4.1 Protéger les biens et les informations mis à disposition

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Il est de la responsabilité de chacun de s'assurer de la protection des biens et des informations qui lui sont confiés et auxquels il a accès.

L'accès au SI ne doit se faire qu'en utilisant les moyens autorisés et/ou mis à disposition par l'AP-HP, sans chercher à les contourner ou à désactiver les mesures de sécurité existantes.

Les principes mis en œuvre par l'AP-HP concernent :

- Le contrôle des accès logiques aux biens et aux données :  
Tout accès au SI nécessite une identification et une authentification personnelle. La constitution des identifiants doit obéir à des règles de construction. Des identifiants non personnels peuvent néanmoins être utilisés dans certains cas particuliers. Ils doivent faire l'objet d'une demande de dérogation limitée dans le temps. L'authentification se base *a minima* sur un mot de passe personnel et incessible respectant des critères de sécurité fixés par la délibération de la CNIL n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.  
L'accès aux données doit être géré tout au long de leur cycle de vie, que ce soit via les accès utilisateurs, les accès administrateurs, mais aussi les interfaces applicatives ou à travers les infrastructures techniques (base de données par exemple).  
Enfin, des contrôles sont effectués régulièrement de manière à repérer et corriger le plus rapidement possible les anomalies (sessions anormalement longues et comptes non utilisés par exemple).
- La protection renforcée des données qui le nécessitent :  
Les données accédées, échangées, au sein d'une entité, entre les entités de l'AP-HP ou avec des tiers sont protégées en fonction de leur niveau de sensibilité et en fonction du niveau d'exposition des infrastructures utilisées (réseau interne, réseau public, Internet...).  
Ainsi des mécanismes ou moyens additionnels, tels que la cryptographie ou l'authentification renforcée, peuvent être mis en œuvre pour l'accès ou l'échange des données qui le nécessitent.
- La protection des accès physiques aux biens sensibles :  
Des moyens doivent être mis en place pour se protéger contre les menaces environnementales (par exemple : incendie, dégât des eaux) et les menaces d'intrusions physiques (par exemple : vol de disques durs contenant des informations sensibles...).

## 3.4.2 Protéger les données par des habilitations adaptées

Tout accès aux données du SI doit donner lieu à une habilitation préalable. À ce titre, un cadre de cohérence commun doit être établi au niveau de l'AP-HP pour la gestion des habilitations. En particulier, un **circuit d'habilitation** (arrivée, départ, mobilité, des agents, des contractuels et des tiers) doit être défini et appliqué.

La gestion globale des habilitations doit respecter le principe de séparation des fonctions et des pouvoirs (décision – mise en application – contrôle).

Les habilitations sont personnelles, liées à l'exercice de la fonction, incessibles et limitées dans le temps. Elles suivent le principe du **besoin d'accès légitime**, c'est-à-dire qu'elles sont définies de manière à autoriser l'accès et l'utilisation des biens au personnel dont l'activité le nécessite. Ainsi, tout changement d'activité doit donner lieu à une suppression et/ou une modification des accès accordés à l'utilisateur concerné.

## Politique Générale de Sécurité du Système d'Information de l'AP-HP

Par ailleurs, l'utilisation des droits d'administration et les droits étendus doivent se limiter exclusivement aux actes d'administration.

Enfin, tout accès au SI accordé à un tiers doit faire l'objet d'une autorisation préalable. En outre, la modification et/ou la suppression des accès doivent faire l'objet d'une procédure appliquée de façon systématique. Par ailleurs, il est important de s'assurer que toutes les exigences de sécurité identifiées sont traitées avant que l'accès aux biens et aux informations de l'AP-HP ne soit donné.

### 3.4.3 Mettre en place une traçabilité des accès

La traçabilité des accès doit être mise en œuvre au regard du niveau de criticité de la ressource considérée et des exigences métiers.

Les traces doivent être définies de manière à pouvoir être corrélées et analysées *a posteriori*.

Elles doivent faire l'objet des différentes déclarations ou informations légales requises, en particulier devant les instances représentatives du personnel.

## 3.5 Protection des infrastructures

Des mécanismes et des moyens de sécurité doivent être mis en œuvre pour fournir un niveau minimum et cohérent de sécurité à l'ensemble du SI de l'AP-HP.

Ces moyens doivent notamment protéger le SI de l'AP-HP des intrusions et/ou des codes malicieux (virus, cheval de Troie, vers...).

Des mécanismes complémentaires peuvent être ajoutés en fonction des enjeux et des risques pour chaque projet SI mené.

### 3.5.1 Protéger le réseau de l'AP-HP

Le réseau de l'AP-HP doit être protégé tout en permettant les échanges métiers.

Afin de protéger de manière spécifique les biens les plus critiques de l'AP-HP, un **principe de cloisonnement des réseaux** doit être défini et mis en œuvre afin d'éviter les rebonds. Ainsi, le réseau de l'AP-HP doit être structuré en « zones de confiance » selon :

- Le niveau de sensibilité et des risques des biens hébergés,
- Le niveau de risque que font peser les utilisateurs qui y accèdent.

À l'intérieur et entre chacune de ces zones, des mesures de sécurité peuvent être mises en place. Il peut s'agir de :

- Contrôle d'accès restrictif,
- Les dispositifs de filtrages sont configurés pour garantir l'acheminement des seuls flux autorisés, transmis par les seuls émetteurs autorisés, aux seuls destinataires devant les recevoir.
- Authentification à l'entrée d'une zone,
- Contrôle de flux échangés (antivirus, filtrage URL, détection d'intrusion),
- Contrôle de conformité.



## Politique Générale de Sécurité du Système d'Information de l'AP-HP

À titre d'exemple, toute interconnexion avec Internet peut faire l'objet d'un filtrage restrictif, d'une authentification, d'un contrôle des flux, et d'un rebond ou d'une rupture protocolaire.

### 3.5.2 Protéger les postes de travail et les serveurs de l'AP-HP

Des moyens complémentaires doivent être mis en place pour protéger les postes de travail et serveurs connectés au réseau de l'AP-HP :

- Les postes de travail sont déployés conformément à des configurations initiales standard, définies par le Département Infrastructure et Services de la DSI.
- Les postes de travail et serveurs sont dotés d'antivirus.
- L'accès à la configuration des postes de travail et des serveurs doit être restreint à des personnes habilitées et formées à cette opération.
- Les règles d'utilisation du poste de travail doivent être définies et formalisées dans une charte d'utilisation du SI de l'AP-HP.

### 3.5.3 Mettre à jour la sécurité des infrastructures

Le niveau de sécurité des infrastructures doit être maintenu à jour. Les mises à jour passent par :

- Un suivi des évolutions des menaces,
- Une veille et identification des vulnérabilités,
- Un maintien à jour des infrastructures par le déploiement des correctifs et des actions de configuration.

### 3.5.4 Mettre en place une traçabilité technique et applicative

L'AP-HP doit disposer d'un mécanisme de gestion des traces approprié permettant de détecter au mieux des événements de sécurité ou de mener une investigation efficace en cas d'incident de sécurité.

Pour chaque SI, les actions suivantes doivent être réalisées :

- Identifier le type de trace, applicative et technique, qui doit être conservé selon la réglementation applicable et en fonction des risques préalablement identifiés auxquels le SI est soumis,  
Ces traces doivent être définies de manière à pouvoir être corrélées et analysées *a posteriori*.
- Préciser les modalités de gestion et de conservation associées et mettre en œuvre le dispositif de traçabilité conformément aux exigences et attendus.

Les traces conservées doivent être exploitables dans la durée.

## 4 ORGANISATION ET INSTANCES DE PILOTAGE

### 4.1 Rôles et responsabilités

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

La mise en œuvre de la sécurité du SI relève de chaque collaborateur en fonction de son niveau de responsabilité et des principes de gouvernance de l'AP-HP.

L'objectif du présent chapitre est de définir et attribuer les principaux rôles et responsabilités en termes de sécurité du SI.

L'organisation de la Sécurité du SI repose sur le principe de la séparation des pouvoirs. Les fonctions de mise en œuvre et de contrôle ne sont pas assumées par les mêmes acteurs.

## 4.1.1 Les Directions des entités

La sécurité du SI couvre un ensemble d'actions assurées par la Direction Générale, les Directions Fonctionnelles, la Direction des Systèmes d'Information et ses départements, les Directions des Groupements Hospitaliers et Hôpitaux hors groupe et les Directions des Pôles d'Intérêt Commun. Elles sont responsables de la sécurité dans leur périmètre et propriétaires de processus qu'elles exploitent, à ce titre :

- Elles ont principalement un rôle d'expression de leurs besoins de sécurité et de validation, *a minima* annuelle, des plans d'actions.
- Elles classifient leurs informations et leurs biens ou, *a minima*, identifient les plus critiques.
- Elles appuient les actions sécurité mises en œuvre. De plus, elles sont actrices dans les actions impactant les utilisateurs dont elles sont responsables, telles que la mise en place des circuits d'habilitation ou la sensibilisation.

En outre, certaines Directions peuvent être particulièrement impliquées dans les actions de sécurité.

- Direction ou service en charge de la mise en œuvre de la sécurité physique des locaux et des salles informatiques,
- Direction ou Service en charge du conseil, d'avis sur sollicitation et de veille sur le volet légal et réglementaire SI,
- Direction ou Service en charge du respect de l'intégration des clauses de confidentialité dans les contrats de travail et/ou dans le règlement intérieur,
- Direction ou Services pouvant acquérir du matériel informatique (service du bio-médical, ou service technique par exemple) : ils doivent travailler en collaboration avec le RSSI de leur périmètre pour s'assurer de la conformité des usages à la présente PGSSI et à toute règle de sécurité du SI édictée par l'AP-HP.

## 4.1.2 Les utilisateurs

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

Est considéré comme « utilisateur » tout agent, titulaire ou contractuel, ou tiers accédant au SI de l'AP-HP.

Tout utilisateur du SI de l'AP-HP se doit de respecter la réglementation et les règles de sécurité en vigueur.

Les conditions d'utilisation du SI sont formalisées dans une Charte d'utilisation du SI et validées par des instances appropriées, de manière à être opposables en cas de nécessité. Pour les utilisateurs collaborateurs d'une société extérieure, elles doivent être précisées dans le contrat avec cette société.

## 4.1.3 La filière Sécurité du Système d'Information de l'AP-HP

### 4.1.3.1 Organisation de la filière sécurité de l'AP-HP

Des actions de sécurité sont spécifiquement portées par la filière sécurité du SI (SSI) de l'AP-HP. Cette filière est constituée de responsables sécurité du SI au sein de la direction des systèmes d'information, des GH/Site/PIC. Cette fonction peut être portée à temps partiel, en fonction du périmètre concerné.

Ces RSSI **sont responsables de la sécurité de leur périmètre** et en sont **garants** vis-à-vis de leur direction et du RSSI de l'AP-HP. Ils travaillent en coordination avec le RSSI de l'AP-HP et sont rattachés hiérarchiquement à leurs Directions respectives.

L'objectif d'une telle organisation est de donner une dynamique à la sécurité du SI de l'AP-HP, de partager et coordonner les actions de sécurité.

Au sein de la filière sécurité SI, la coordination passe, outre les échanges bilatéraux, par un reporting régulier auprès du RSSI de l'AP-HP.

### 4.1.3.2 Rôles des responsables sécurité du SI

Ce chapitre présente les rôles et responsabilités des différents RSSI de la filière Sécurité du SI.

#### Le RSSI AP-HP :

Le RSSI de l'AP-HP est rattaché hiérarchiquement au directeur des systèmes d'information de l'AP-HP.

Le RSSI de l'AP-HP est garant du respect de la présente politique. À ce titre, il assure la gouvernance et le pilotage de la sécurité à l'échelle de l'AP-HP, en fixant les priorités par rapport aux moyens dont il dispose. Il doit notamment :

- **Identifier les risques majeurs et transverses** à l'AP-HP annuellement, consolider les indicateurs en centralisant les reportings transmis par les RSSI de chaque entité, et définir les **plans d'actions transverses de traitement des risques**, en collaboration étroite avec les RSSI de la filière,
- **S'assurer du bon déroulement des plans d'actions définies**
- **Diffuser la PGSSI** et les directives de sécurité auprès de toutes les entités de l'AP-HP et proposer sa mise à jour aux comités de pilotage infrastructure et sécurité afin d'intégrer tout besoin significatif d'évolution,
- Contrôler l'efficacité des mesures en définissant un **plan d'audits réguliers** réalisables sur l'ensemble du périmètre AP-HP et de ses partenaires, et en présentant une restitution des audits au comité de suivi de la sécurité des systèmes d'information.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

- **Porter les projets de sécurité transverses** tels que la sensibilisation des utilisateurs des systèmes d'information (qu'ils soient internes ou externes), la gestion des habilitations et le plan de secours informatique,
- Contribuer aux actions **de veille sécurité**, particulièrement au sujet des menaces et vulnérabilités en relation étroite avec les RSSI de chaque entité et les autorités et organismes externes (groupes de réflexion, etc.),
- Assurer la définition, le suivi et la consolidation des **tableaux de bord de sécurité des SI**,
- Disposer d'une vision transverse des budgets, et **valider les budgets consolidés des projets sécurité transverses**,
- Animer la filière sécurité SI de l'AP-HP,
- Assurer la préparation et l'animation des comités dédiés à la sécurité des systèmes d'information.
- Instruire les **demandes de dérogations** à la PGSSI de l'AP-HP en définissant une date de fin, et en en référant au comité de suivi de la sécurité des systèmes d'information si besoin,
- Contribuer à l'émission des besoins relatifs aux solutions de sécurité,
- Exercer un **rôle de support** auprès des différentes entités,
- Représenter l'AP-HP dans les groupes de réflexion externes (ASIP ou ANSSI par exemple).

## Le RSSI du Département Infrastructure et Services de la DSI :

Le RSSI DIS est un responsable de la sécurité opérationnelle des infrastructures de l'AP-HP. Il apporte le support aux chefs de projet DIS dans l'identification et la mise en œuvre des mesures de sécurité en les priorisant par rapport aux moyens dont il dispose. Il doit notamment :

- Préciser les mesures et moyens existants dans le contrat de service : Plan de secours informatique, Protection antivirale, Isolation réseau...,
- Piloter la mise en œuvre des actions de sécurité des infrastructures,
- Remonter les indicateurs mis en place et les incidents de sécurité rencontrés aux RSSI concernés, et au RSSI de l'AP-HP pour ceux qui sont communs à plusieurs entités :
  - Assurer le reporting des informations liées à la sécurité au RSSI de l'AP-HP (indicateurs, incidents, résultat de l'analyse de risques...),
  - En particulier transmettre les risques majeurs identifiés sur le périmètre et les plans d'actions de traitement des risques avant mise en œuvre,
  - Les estimations budgétaires liées au plan d'action de traitement des risques défini devront être transmises au RSSI de l'AP-HP.
- Apporter, dans le cadre de l'intégration de la sécurité dans les projets, le **support aux chefs de projet du DIS** dans l'identification et la mise en œuvre des mesures de sécurité,
- S'assurer de **l'inscription à l'ordre du jour de la sécurité dans les instances de pilotage** de leur périmètre et participer à ces instances,
- Formaliser et mettre en place un processus de **veille sécurité technique**,
- S'assurer de la **gestion et du contrôle des habilitations des applications / systèmes / équipements de leur périmètre** :
  - Contribuer à la définition et valider les matrices d'habilitations (profils et droits associés), en conformité aux risques, aux enjeux et à la réglementation applicable ;

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

- Effectuer un contrôle de niveau 1 des habilitations du personnel SI de son périmètre (notamment pour les comptes à privilèges d'exploitation),
- Effectuer un contrôle de niveau 2 des habilitations : vérifier la réalisation des contrôles par les responsables métiers et contrôler les incohérences,
- Décliner les **actions de sensibilisation** de façon à ce que tout utilisateur des SI de leur périmètre prenne connaissance des bonnes pratiques de sécurité à respecter.

## Les RSSI des départements Gestion, Patient et WIND de la DSI :

Les RSSI des départements sont en charge de la déclinaison opérationnelle de la PGSSI sur leur périmètre, en priorisant les actions par rapport aux moyens dont ils disposent :

- Définir annuellement un **plan d'actions** dans le domaine de la sécurité des SI sur leur périmètre au regard des risques et des enjeux,
- Assurer **la remontée d'informations** au RSSI de l'AP-HP pour une coordination des actions de sécurité et une identification des actions transverses :
  - Assurer le reporting des informations liées à la sécurité au RSSI de l'AP-HP (indicateurs, incidents, résultat de l'analyse de risques...),
  - En particulier transmettre les risques majeurs identifiés sur le périmètre et les plans d'actions de traitement des risques,
  - Les estimations budgétaires liées au plan d'action de traitement des risques défini devront être transmises au RSSI de l'AP-HP.
- **Piloter** les projets sécurité liés à leur périmètre,
- Valider les évolutions des mesures de sécurité existantes sur leur périmètre et participer à la mise à jour du plan de secours informatique,
- **S'assurer de l'intégration de la sécurité dans les projets** de nouvelles applications ou de maintenance évolutive (définition des besoins, analyse de risques, identification des mesures de sécurité à mettre en œuvre, recettes, évolution) en apportant le **support** nécessaire **aux chefs de projets**,
- S'assurer de **l'inscription à l'ordre du jour de la sécurité dans les instances de pilotage** de leur périmètre, notamment le COPIL du domaine concerné et les COPIL de projet ; et participer à ces instances,
- Assurer une veille sécurité sur son périmètre et en partager les éléments clés avec la filière Sécurité du SI,
- S'assurer de la **gestion et du contrôle des habilitations des applications / systèmes / équipements de leur périmètre** :
  - Contribuer à la définition et valider les matrices d'habilitations (profils et droits associés), en conformité aux risques, aux enjeux et à la réglementation applicable ;
  - Effectuer un contrôle de niveau 1 des habilitations du personnel SI de son périmètre,
  - Effectuer un contrôle de niveau 2 des habilitations : vérifier la réalisation des contrôles par les responsables métiers et contrôler les incohérences,
- Décliner les **actions de sensibilisation** de façon à ce que tout utilisateur des SI de leur périmètre prenne connaissance des bonnes pratiques de sécurité à respecter.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

## Les RSSI GH/Site/PIC :

Les RSSI des GH/Site/PIC sont garants du bon déploiement de la PGSSI au sein de leur groupe hospitalier. Ainsi, ils travaillent conjointement avec les autres RSSI de la filière pour mettre en œuvre les mesures de sécurité identifiées (sécurité des réseaux filaire, des postes de travail, etc.), en priorisant ces mesures par rapport aux moyens dont ils disposent. À ce titre, ils doivent notamment :

- **Décliner** les plans d'actions sécurité en mettant en œuvre les mesures définies par le RSSI AP-HP pour les sujets transverses, le RSSI DIS pour les infrastructures (réseaux, postes de travail) ou les RSSI départements Gestion, Patient ou WIND de la DSI pour les applications,
- **Identifier les actions locales** complémentaires de sécurisation du SI et les formaliser dans un plan d'action chiffré, **le communiquer aux RSSI concernés** pour l'identification des actions transverses et le mettre en œuvre,
- Assurer **la remontée d'informations** au RSSI de l'AP-HP pour une coordination des actions de sécurité :
  - Assurer le reporting des informations liées à la sécurité au RSSI de l'AP-HP (indicateurs, incidents, résultat de l'analyse de risques...),
  - En particulier transmettre les risques majeurs identifiés sur le périmètre et les plans d'action de traitement des risques,
  - Les estimations budgétaires liées au plan d'action de traitement des risques défini devront être transmises au RSSI de l'AP-HP.
- Capitaliser autour des modes dégradés de fonctionnement sans informatique (dans le cadre des plans de continuité d'activités).
- S'assurer de **l'inscription à l'ordre du jour de la sécurité dans les instances de pilotage** de leur périmètre, notamment les réunions informatiques réalisées au sein de son GH ; et participer à ces instances,
- S'assurer de la **gestion et du contrôle des habilitations des applications / systèmes / équipements de leur périmètre** :
  - Contribuer à la définition et valider les matrices d'habilitations (profils et droits associés), en conformité aux risques, aux enjeux et à la réglementation applicable ;
  - Effectuer un contrôle de niveau 1 des habilitations du personnel SI de son périmètre,
  - Effectuer un contrôle de niveau 2 des habilitations : vérifier la réalisation des contrôles par les responsables métiers et contrôler les incohérences,
- Décliner les **actions de sensibilisation** de l'AP-HP de façon à ce que tout utilisateur des SI de leur périmètre prenne connaissance des bonnes pratiques de sécurité à respecter.

## 4.2 Instances de pilotage

### 4.2.1 Comités dédiés à la sécurité SI

Afin d'animer la démarche sécurité au sein de l'AP-HP, des instances complémentaires, dédiées à la SSI sont mises en place :

Comités dédiés à la	Présidence	Fréquence	Ordre du jour
---------------------	------------	-----------	---------------

## Politique Générale de Sécurité du Système d'Information de l'AP-HP

sécurité des SI			
<b>Comité de pilotage Infrastructures et Sécurité des Systèmes d'Information</b>	Présidé par le Secrétaire Général	Fréquence semestrielle	Dédié au suivi des risques majeurs et du plan de traitement associé
<b>Comité de Suivi de la Sécurité des Systèmes d'information</b>	Présidé par le Directeur des Systèmes d'information	Fréquence trimestrielle	<ul style="list-style-type: none"> <li>• Avancement des plans d'action sécurité</li> <li>• Indicateurs</li> <li>• Suivi des budgets SSI</li> <li>• Suivi des incidents SSI</li> <li>• Restitutions d'audits liés à la SSI</li> </ul>
<b>Comité RSSI</b>	<b>Composé de l'ensemble des RSSI de l'AP-HP.</b>	Fréquence mensuelle	<ul style="list-style-type: none"> <li>• Indicateurs</li> <li>• Présentation des initiatives de sécurité et capitalisation</li> <li>• Présentation et suivi des projets transverses</li> <li>• REX incidents</li> <li>• Identification des actions transverses à entreprendre</li> </ul>

### 4.2.2 Comités SI durant lesquels la sécurité est inscrite à l'ordre du jour

Outre ces trois comités consacrés à la SSI, il existe d'autres instances de pilotage non dédiées à la SSI dont la sécurité doit être inscrite à l'ordre du jour :

## Politique Générale de Sécurité du Système d'Information de l'AP-HP

Comités SI durant lesquels la sécurité doit être inscrite à l'ordre du jour	Participants SSI	Ordre du jour lié à la sécurité SI
<b>CODIR DSI élargi</b>	Permanent : RSSI AP-HP	Actualités sécurité SI : focus sur un chantier sécurité en cours, partage d'un incident de sécurité...
<b>COPIL Infrastructures et Sécurité</b>	Permanents : SSI AP-HP Invités/informés : RSSI des départements de la DSI ; RSSI GH	<ul style="list-style-type: none"> <li>■ Suivi des activités sécurité : antivirus, gestion des correctifs de sécurité, alertes et incidents sécurité</li> <li>■ Avancement des plans d'action sécurité DIS et GH</li> </ul>
<b>COPIL SI de domaine : COPIL SI Patient, COPIL SI Gestion, COPIL Projet</b>	Permanents : RSSI département concerné Invités/informés : RSSI APHP, RSSI GH	<ul style="list-style-type: none"> <li>■ Suivi de la prise en compte de la sécurité dans les projets : présentation des enjeux de sécurité et des exigences à mettre en œuvre,</li> <li>■ Gestion et contrôle des habilitations</li> <li>■ Partage des incidents de sécurité sur le périmètre</li> <li>■ Avancement des plans d'action sécurité sur le périmètre</li> </ul>
<b>Réunion informatique propre à chaque GH</b>	Permanent : RSSI GH du GH concerné	<ul style="list-style-type: none"> <li>■ Suivi des activités sécurité au sein d'un GH</li> <li>■ Avancement des plans d'action sécurité sur le périmètre</li> <li>■ Partage de l'actualité sécurité</li> </ul>



## 5 GLOSSAIRE

**Analyse de risque** : Processus visant à identifier les risques, déterminer leur impact et leur probabilité d'occurrence et définir les mesures de sécurité nécessaires.

**Audit** : Opération visant à analyser les actions effectuées sur des données ou des biens ou à mesurer l'écart par rapport à un référentiel (par exemple la PGSSI) ou par rapport à l'état de l'art.

**Bien** : Élément unitaire (logiciel, matériel, service) sur lequel s'applique la PGSSI de l'AP-HP.

**CIL** : Correspondant Informatique et Libertés (CIL).

**Cloisonnement** : Principe consistant à confiner des biens du SI dans des zones de sécurité spécifiques (ou segment réseau) et à contrôler les communications entre les biens situés sur des zones de sécurité distinctes.

**Commanditaire** : Entité faisant la demande d'un projet. Elle est donc à l'origine du lancement du projet, et valide du résultat de celui-ci (applications ou services par exemple).

**Confidentialité** : Un des critères de sécurité permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder.

**Contrôle d'accès** : Fonctionnalité de sécurité visant à autoriser l'accès à un bien ou un traitement en fonction de l'identifiant et l'authentifiant fournis et des droits associés.

**Contrôle des habilitations de niveau 1** : auto contrôle et/ou du contrôle hiérarchique de la bonne réalisation d'une activité, par exemple vérification des habilitations réalisées sur le périmètre de responsabilité

**Contrôle des habilitations de niveau 2** : vérification par une personne indépendante de la réalisation des contrôles de niveau 1.

**Délai d'Interruption Maximal Admissible (DIMA)** : Durée maximale d'interruption d'une ressource que peuvent tolérer les Métiers utilisateurs de la ressource. On parle également de Recovery Time Objective (RTO).

**DIS** : Département Infrastructure et Services de la DSI.

**Disponibilité** : Un des critères de sécurité, aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues.

**Droits d'accès** : Ensemble de droits accordés sur une ressource, permettant d'effectuer des actions sur celle-ci (création, consultation, modification, suppression).

**DSIG** : Département Système d'Information Gestion de la DSI.

**DSIP** : Département Système d'Information Patient de la DSI.

**Externalisation des sauvegardes** : Opération consistant à transférer tout ou partie des données sauvegardes vers un site autre que celui hébergeant lesdites données.

**Habilitation** : Attribution à un utilisateur de droits d'accès à des biens informatiques par une entité autorisée.

**Incidents de sécurité** : on appelle incident de sécurité des systèmes d'information tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information de l'AP-HP.

# Politique Générale de Sécurité du Système d'Information de l'AP-HP

**Intégrité** : Un des critères de sécurité, garantie de l'exactitude, de la fiabilité et de l'exhaustivité des informations et des méthodes de traitement.

**Métier** : Appellation désignant un domaine d'activité de l'AP-HP correspondant à des compétences et savoir-faire homogène (exemples : Patient, Finance, Ressources humaines).

**Niveau de criticité** : Quantification de l'importance des critères de sécurité DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité) selon une échelle de valeurs prédéfinies.

**Partenaire** : Entité externe qui intervient en liaison avec l'AP-HP sur un domaine donné (exemple : les associations).

**Perte de Données Maximale Admissible (PDMA)** : Durée maximale acceptable entre la dernière sauvegarde et l'incident survenu, quantifiant ainsi les données que les Métiers tolèrent de perdre au maximum. On parle également de Recovery Point Objective (RPO).

**PGSSI** : Politique Générale de Sécurité des Systèmes d'Information.

**Propriétaire de processus** : Il s'agit d'une entité ou d'une personne responsable du bon fonctionnement du processus concerné, notamment des fonctions SI supportant le processus.

**Risque** : Scénario de réalisation d'une menace à travers une ou plusieurs vulnérabilités. Exprimé sous la forme d'un impact et d'une probabilité d'occurrence.

**Sauvegarde** : Copie périodique des données d'un système sur un support pouvant être mis hors ligne et stocké hors du site de production, afin de permettre la récupération des données après incident ou sinistre.

**Sous-traitant** : Entités ou organismes externes en relation contractuelle avec l'AP-HP. Le sous-traitant travaille à la demande et sous le contrôle de l'AP-HP.

**Système d'information** : ensemble organisé de ressources (données, procédures, matériel, logiciel, personnel, etc.) permettant d'acquérir, traiter, stocker, diffuser ou détruire les informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des informations (numérique, papier, oral, etc.).

**Tiers** : Entités ou organismes externes en relation contractuelle avec l'AP-HP. Sont ainsi considérés comme des tiers : les prestataires, les intérimaires, les partenaires...

**Traçabilité** : Un des critères de sécurité, ce critère traduit la garantie que les événements et les accès sont enregistrés à travers des traces accessibles et si besoin, opposables.

**Trace** : Elle permet de suivre les traitements réalisés sur les informations au sein des processus et de mener des analyses *a posteriori*.

**Utilisateur** : Désigne toute personne susceptible de pouvoir accéder au SI de l'AP-HP. Sauf mention contraire, désigne également les administrateurs, les exploitants et les prestataires externes intervenant sur le SI.

**WIND** : Département WEB Innovation et Données de la DSI.