

Politique Générale de Sécurité de l'information de l'AP-HP

1.2

C0 – Public

En cours

Table des matières

1	LETTRE D'ENGAGEMENT DE LA DIRECTION	3
2	INTRODUCTION	4
3	OBJECTIFS STRATEGIQUES DE SECURITE	7
4	ORGANISATION GENERALE DE LA SECURITE	8
5	CORPUS DOCUMENTAIRE	11
	ANNEXE 1 : GLOSSAIRE DE LA SECURITE	13
	ANNEXE 2 : RESSOURCES ALLOUEES A LA SECURITE	16
	ANNEXE 3 : OBLIGATIONS LEGALES ET REGLEMENTAIRES	17
	ANNEXE 4 : INSTANCES DE PILOTAGE DE LA SECURITE	18

Référence	PO_AP-HP - PGSI V1.2.docx
Prochaine mise à jour	2025
Durée d'utilité administrative	5 ans
Responsable	Didier PERRET – RSSI
Approbateur	Raphaël BEAUFRET- DSN de l'AP-HP

Suivi des versions			
Version	Date	Auteur	Objet
1.0	16/09/2022	PERRET D.	Validation de la PGSI lors du COSTRAT de septembre 2022.
1.1	11/05/2023	PERRET D.	Actualisation 2023. Prise en compte du centre support unifié. Traitement de la non-conformité mineure 2304-MIN03 (Cf. ANNEXE 4 : INSTANCES DE PILOTAGE DE LA SECURITE)
1.11	06/04/2024	PERRET D.	Changement de directeur pour la DSN
1.2	05/11/2024	PERRET D.	Revue 2024

1 LETTRE D'ENGAGEMENT DE LA DIRECTION

Ces dernières années ont été marquées par un accroissement et une évolution de la menace sur les services numériques parallèlement à une extension des surfaces d'attaques dans les GHU/Site/PIC de l'AP-HP. Pour y faire face, deux approches complémentaires doivent être menées.

Grands Principes de Sécurité Numérique

La disponibilité :

Les SN de l'AP-HP doivent remplir ses fonctions dans des conditions prédéfinies d'horaire et de délai.

L'intégrité :

Les SN de l'AP-HP doivent garantir l'exhaustivité, la validité et la cohérence des informations.

La confidentialité :

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

Le premier axe stratégique doit prendre en compte de façon transverse les enjeux de conformité et de souveraineté dans le domaine numérique. L'AP-HP est en effet un opérateur incontournable de la Santé du pays et le premier employeur d'Ile de France. La protection de ses services numériques face à la menace cyber et aux éventuelles tentatives de déstabilisation des états étrangers engage la préservation des intérêts de la France et de ses citoyens tant d'un point de vue économique que sanitaire. Dans ce contexte, la donnée, son utilisation et sa protection, doit être au centre de la réflexion sur la sécurité numérique. Par ailleurs, la conformité à l'important corpus légal et réglementaire applicable aux structures hospitalières permet de confirmer la volonté de s'inscrire dans une démarche souveraine.

Le second axe stratégique porte sur la cyber-résilience, c'est-à-dire la capacité des établissements à assurer leurs missions de service public quoi qu'il arrive. La prise de conscience de la dépendance vis-à-vis des technologies du numérique invite à anticiper toute compromission ou perte de disponibilité des services et des données et à se préparer à réagir en cas d'attaque à travers un ensemble de moyens de détection, de gestion des incidents et de gestion de crise.

Que ce soit pour se protéger, se défendre ou pour préparer sa cyber-résilience, l'AP-HP se dote des outils techniques et de gouvernance pour anticiper les attaques, identifier leurs sources et les potentiels impacts sur les patients et les services de l'AP-HP. Enfin, la fiabilité et la confiance dans la technologie passent également par la capacité de la DSN de proposer à ses agents des services numériques simples d'utilisation et répondant à leurs

besoins, mais aussi par la pédagogie. L'AP-HP a ainsi à cœur de maintenir les compétences nécessaires pour assurer sa sécurité à travers des formations ou des sensibilisations spécifiques aux usages numériques des différents métiers.

La Sécurité de l'information de l'AP-HP est formalisée dans un référentiel documentaire dont la présente Politique Générale de l'Information constitue le premier niveau, fixant les principes de sécurité et les orientations stratégiques de l'organisation. Elle constitue le référentiel général en lien avec le schéma directeur 2021-2025.

2 INTRODUCTION

2.1 Contexte

La [Politique Générale de Sécurité de l'Information](#) (PGSI) a pour objectif de fournir un cadre de référence et de cohérence à la Sécurité de l'information de l'AP-HP en conformité avec la PGSSI Santé. 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 des Services Numériques (SN).

2.2 S'aligner aux enjeux stratégiques des Services Numériques de l'AP-HP

La Sécurité du SN doit être en phase avec les objectifs stratégiques fixés pour le SN de l'AP-HP dans le cadre du plan stratégique 2021-2025 et du schéma directeur des Services Numériques de l'AP-HP pour la période 2021-2025.

La PGSI prend en compte les perspectives identifiées dans le plan stratégique, qui elles-mêmes se déclinent dans le schéma directeur des services numériques en 5 axes stratégiques :

Axe 1 : Les SN au service des parcours de prise en charge des patients, de l'organisation et des services supports

Axe 2 : la donnée pour accompagner la recherche et l'innovation

Axe 3 : le soutien au pilotage et aux projets stratégiques

Axe 4 : la performance des SN

Axe 5 : l'organisation de la DSN.

La PGSI et son référentiel documentaire développent notamment le principe de souveraineté numérique et la cybersécurité par conception afin de garantir à l'AP-HP la pleine maîtrise de ses processus et données et contribue aux autres principes directeurs du schéma directeur des services numériques.

2.3 Périmètre d'application

La PGSI s'applique à l'ensemble de l'AP-HP : la Direction Générale, les Directions Fonctionnelles, les Groupes Hospitalo-universitaires (GHU), les hôpitaux hors groupes (Site), les Pôles d'Intérêt Commun (PIC) et la Direction des Services Numériques (DSN).

La PGSI s'applique aussi aux entités sous-traitantes et aux partenaires externes accédant aux SN 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 PGSI sur le périmètre d'actions impactant les SN 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 PGSI sur le périmètre des SN commun avec l'AP-HP.

Les SN sont considérés 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 PGSI s'applique aux usages impliquant une interaction avec les SN 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 PGSI couvre les services numériques 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.

2.4 Cadre de référence

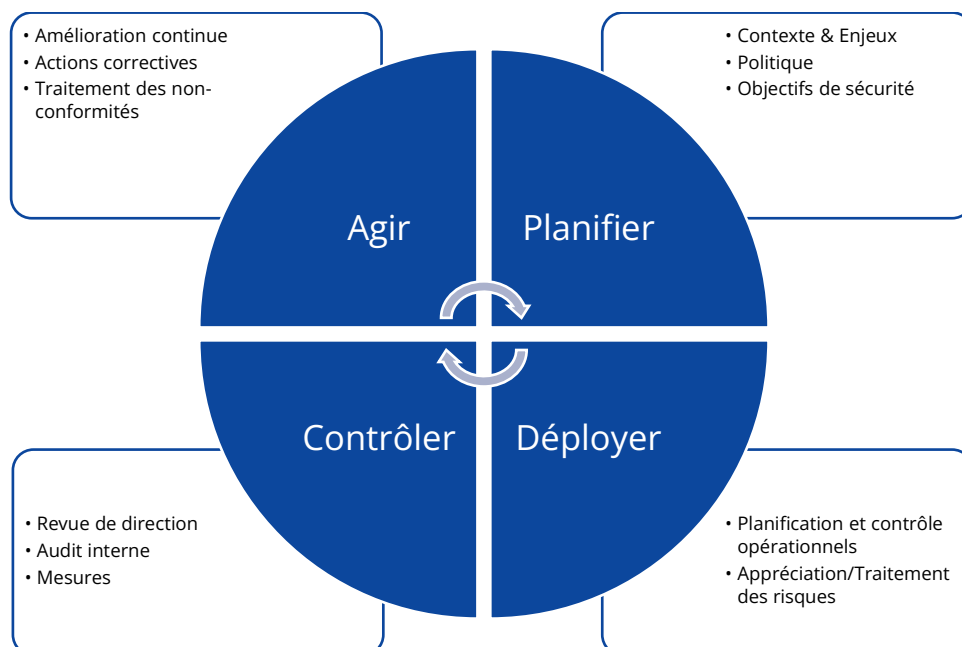
La Sécurité des SN de l'AP-HP est formalisée dans un référentiel documentaire dont la présente [Politique](#) constitue le premier niveau, fixant les principes de sécurité et les orientations d'organisation (Cf. CORPUS DOCUMENTAIRE CORPUS DOCUMENTAIRE à la page N°11 et suivantes).

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 (Annexe n°16).

2.5 Inscrire la sécurité dans un cycle d'amélioration continue

La Sécurité de l'AP-HP est inscrit dans une démarche d'amélioration continue, mettant en œuvre la [norme internationale de gestion de la sécurité de l'information ISO/IEC 27001:2017](#).

La DSN est déjà [certifiée ISO27001](#) et [HDS](#) pour une part de ses services (Référence AFNOR N° 2020/87844.3). Elle étendra progressivement le périmètre certifié à l'ensemble des Services Numériques.



L'objectif d'une telle démarche est d'apporter des résultats concrets, mesurables et proportionnés aux risques.

2.6 Évolution de la PGSI

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

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

- Les réorganisations (mise en place d'une nouvelle structure impactant les SN par exemple),
- Les évolutions significatives des SN 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 PGSI 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 des SN de l'AP-HP, les révisions et les versions successives qu'il soumet aux instances de pilotage appropriées pour validation.

3 OBJECTIFS STRATEGIQUES DE SECURITE

Pour faire face à la menace cyber et assurer l'alignement sur le schéma directeur des Services Numériques, l'AP-HP définit 8 objectifs stratégiques de la sécurité de l'information présentés ci-dessous.

Gouvernance

Garantir un alignement de la gestion de la sécurité de l'information avec les objectifs et les besoins métiers.

Qualité & Conformité

Inscrire la sécurité dans une démarche d'amélioration continue pour garantir la performance des mesures et des activités de la gestion de la sécurité.

Sensibilisation & Formation

Sensibiliser et former les utilisateurs des SN à la sécurité de l'information

Sécurité dans les projets

Assurer la sécurité par défaut et par conception des projets en adaptant les mesures de sécurité aux risques identifiés

Gestion identités & accès

Maîtriser et sécuriser l'accès aux Services Numériques

Protection de la donnée

Adapter les règles de sécurité à la sensibilité de la donnée

Sécurité opérationnelle

Limiter la survenance des incidents de sécurité

Cyber-résilience

Limiter l'impact des incidents de sécurité en assurant la continuité des activités informatiques en cas de situation exceptionnelle

Ces 8 objectifs stratégiques sont déclinés en objectifs opérationnels pilotés par des indicateurs revus en lors des comités de pilotage stratégique de la sécurité de l'information.

4 ORGANISATION GENERALE DE LA SECURITE

L'organisation de la Sécurité des SN 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 intervenants.

4.1 Les Directions

Les directions (DG, Directions Fonctionnelles, Direction des Services Numériques, Directions des Groupements Hospitalo-Universitaire et Hôpitaux hors groupe et les Directions des Pôles d'Intérêt Commun) sont responsables de la sécurité de l'information sur leur périmètre. A ce titre, elles définissent les besoins de sécurité, la classification des informations, valident et appuient les plans d'actions.

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 en matière de services numériques
- 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 en charge des marchés publics
- Direction ou Services pouvant acquérir du matériel informatique, des logiciels ou des services numériques.

Les missions de la Direction des Services Numériques (DSN) en matière de sécurité de l'information sont détaillées dans la directive « Organisation de la sécurité de l'information ».

4.2 Rôles et responsabilités des utilisateurs

Est considéré comme « Utilisateur » des services numériques toute personne disposant d'un accès logique ou physique aux SN de l'AP-HP quel que soit son statut : agent titulaire ou contractuel, stagiaire, fournisseurs, tiers...

Tout Utilisateur a un rôle à jouer dans la sécurité des services numériques d'information et doit acquiescer les bonnes pratiques d'utilisation. Ils se doivent de respecter la réglementation et l'ensemble des règles de sécurité inscrites dans la Charte de Bon Usage du Système d'Information, annexée au Règlement Intérieur de l'AP-HP.

Pour les tiers (patients, partenaires, fournisseurs, professionnels de santé...), en plus du règlement intérieur, les règles de sécurité doivent être complétées dans les marchés publics, les conventions, les conditions générales d'utilisation... en fonction des risques et des enjeux.

En cas de suspicion d'incident de sécurité, les Utilisateurs doivent contacter le support informatique par mail à l'adresse ✉ assistance.informatique.aphp@aphp.fr ou par téléphone en composant *75 ou depuis l'extérieur (télétravail, structures hors AP-HP) en composant 01 40 27 40 00.

4.3 Rôles et responsabilités des personnels chargés de la mise en œuvre des SN

Les personnels chargés de la mise en œuvre des SN se doivent de respecter les règles applicables aux utilisateurs des SN.

Les conditions de gestion des SN sont formalisées dans une Charte d'administration des SN faisant l'objet d'un engagement individuel. Pour les titulaires de marché publique ou de convention accédant aux SN de l'AP-HP ainsi qu'à tout opérateur économique intervenant pour leur compte, elles doivent être précisées dans le marché publique ou la convention.

4.4 La filière Sécurité des Services Numériques de l'AP-HP

Des actions de sécurité sont spécifiquement portées par la filière sécurité des services numériques de l'AP-HP. Cette filière est constituée de responsables sécurité des SI au sein des Groupes Hospitalo-universitaires (GHU) et des hôpitaux hors groupes (Site). 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 des SN de l'AP-HP, de partager et coordonner les actions de sécurité.

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

4.4.1 Le RSSI AP-HP et son pôle

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 les priorisant par rapport aux moyens dont il dispose. Il doit notamment :

- Identifier les risques de sécurité majeurs et transverses à l'AP-HP et définir les plans d'actions transverses de traitement
- Préparer à la gestion de crise CYBER.
- Diffuser, mettre à jour la politique générale de sécurité de l'information (PGSI) et contrôler son application et son efficacité en définissant un plan d'audits
- Mettre en œuvre et améliorer le système de management de la sécurité de l'information (SMSI) conformément aux exigences de la norme NF/ISO 27001
- Porter les projets de sécurité transverses tels que la sensibilisation des utilisateurs des SI, la gestion des habilitations
- Rendre compte régulièrement à la Direction de la performance sécuritaire et notamment celle du SMSI
- Assurer la fonction de référent pour la certification des comptes
- Assurer la préparation et l'animation des comités dédiés à la sécurité des systèmes d'information, contribuer aux autres COPIL de la DSN, contribuer au schéma directeur des SI
- Développer la démarche d'intégration de la sécurité dans les projets en lien avec la gestion des projets
- Accompagner le délégué à la protection des données dans la rédaction des AIPD, la revue des contrats et l'audit des sous-traitants pour garantir la conformité aux méthodologies de référence de la CNIL
- Mettre en œuvre des outils de surveillance en temps réel pour détecter et réagir rapidement aux menaces de sécurité.
- Assurer la veille sécurité (menaces, vulnérabilités) en collaboration avec les autorités

- Animer la filière sécurité SI de l'AP-HP
- Exercer un rôle de support auprès des différentes entités
- Représenter l'AP-HP dans les groupes de réflexion externes (ANS ou ANSSI par exemple)

4.4.2 Les RSSI GHU/Site/PIC

Les RSSI des GHU/Site sont garants du bon déploiement de la présente Politique au sein de leur entité. Ainsi, ils travaillent conjointement avec le RSSI de l'AP-HP 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
- Identifier les actions locales complémentaires de sécurisation des SN et les formaliser dans un plan d'actions chiffré, le communiquer au RSSI de l'AP-HP 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'actions de traitement des risques,
 - Les estimations budgétaires liées au plan d'actions 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 GHU/Site ; 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 des habilitations du personnel des SN de son périmètre
 - Vérifier la réalisation des contrôles sur les habilitations des utilisateurs des SN par les responsables métiers et contrôler les incohérences.
- Décliner les actions de sensibilisation de l'AP-HP de façon que tout utilisateur des SN de leur périmètre prenne connaissance des bonnes pratiques de sécurité à respecter.

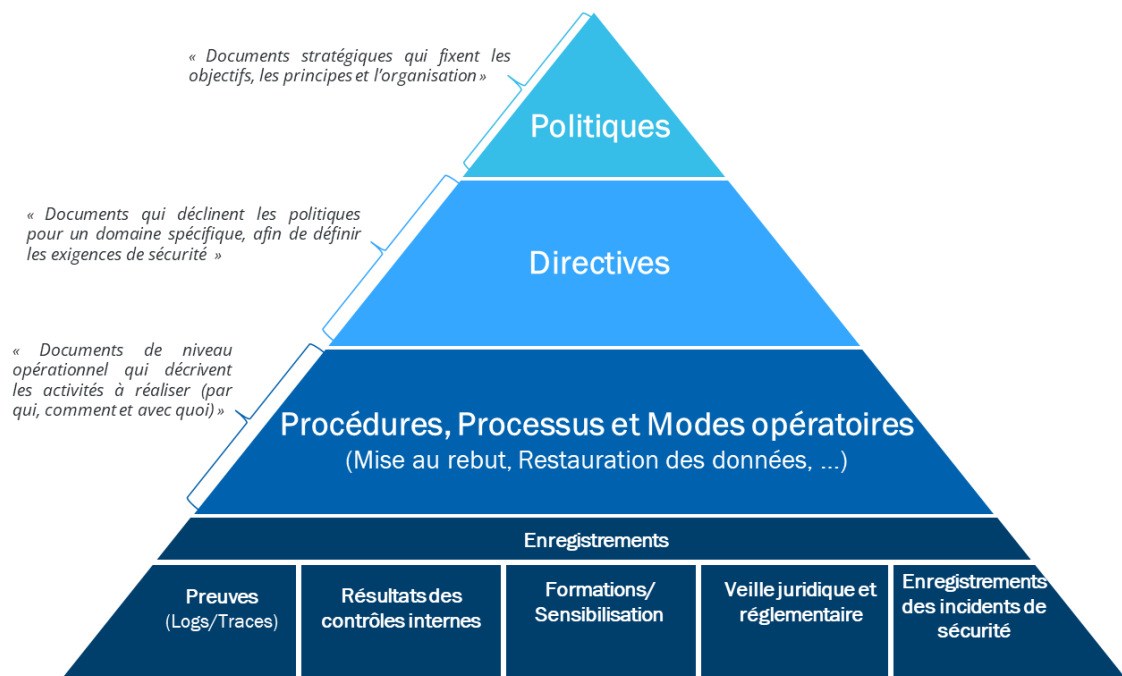
5 CORPUS DOCUMENTAIRE

La documentation destinée aux utilisateurs des services numériques est accessible depuis l'intranet <https://aphp-pro.aphp.fr/SitePages/Home.aspx> rubrique « EXPERTISES ET FONCTIONS SUPPORTS » puis « SYSTEME D'INFORMATION » et « LA SECURITE INFORMATIQUE ».

Il s'agit des bonnes pratiques de sécurité, de sensibilisation, d'actualités autour de la sécurité et de la conduite à tenir lors de la survenance d'un d'incident de sécurité.

La documentation destinée aux professionnels de l'informatique, maitrise d'ouvrage, maitrise d'œuvre, prestataires, acheteurs, personnels chargés de la mise en œuvre des services numériques... est regroupées dans un espace dédié accessible depuis <https://365aphp.sharepoint.com/sites/GDNDN/SitePages/ProjectHome.aspx>.

Elle suit les principes du management de la qualité en adoptant la hiérarchie documentaire suivante :



Les directives couvrent les thématiques de l'annexe A de la norme NF ISO/CEI 27001:2017 :

1. Organisation de la sécurité de l'information
2. Sécurité des Ressources Humaines
3. Gestion des actifs
4. Sécurité des accès logiques
5. Cryptographie
6. Sécurité physique et environnementale
7. Sécurité liée à l'exploitation
8. Sécurité des communications
9. Acquisition, développement & maintenance des systèmes d'information
10. Sécurité dans les relations avec les fournisseurs
11. Gestion des incidents liés à la sécurité de l'information
12. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
13. Conformité des systèmes de traitement de l'information

ANNEXE 1 : GLOSSAIRE DE LA SECURITE

Administrateur : Utilisateur assurant le fonctionnement et l'exploitation d'un ou plusieurs systèmes et disposant à ce titre d'accès étendus et élevés.

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 PGSI) ou par rapport à l'état de l'art.

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

Cloisonnement : Principe consistant à confiner des biens des SN 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).

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.

DPO : DATA PROTECTION OFFICER (ou DPD : Délégué à la Protection des Données) ; il veille au respect du cadre légal concernant la protection des données au sein d'une organisation.

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

DSN : Direction des Services Numériques

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 services numériques tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes 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).

PGSI : Politique Générale de Sécurité de l'Information

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

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

Résilience (Cyber-résilience) : Capacité à retrouver ses capacités d'origine après une perturbation extérieure ou une altération de son environnement. En cybersécurité, il s'agit de la capacité d'un système ou d'une organisation à continuer de fonctionner en s'adaptant malgré des cyber événements indésirables.

RGPD : Règlement Général sur la Protection des Données. Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

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.

RSSI : Responsable de la Sécurité des Systèmes d'Information

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.

Services Numériques : 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.).

SDS N : Schéma Directeur des Services Numériques

SDSSN : Schéma Directeur de la Sécurité des Services Numériques

SSN : Sécurité des Services Numériques

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 aux SN de l'AP-HP. Sauf mention contraire, désigne également les administrateurs, les exploitants et les prestataires externes intervenant sur les SN.

ANNEXE 2 : RESSOURCES ALLOUEES A LA SECURITE

En cible de SDSN 2021-2025, le budget alloué à la sécurité de l'information représente :

- Investissement : $\approx 5,5$ % du budget d'investissement de la DSN consacré à la sécurité
- Fonctionnement : $\approx 5,5$ % du budget de fonctionnement de la DSN consacré à la sécurité

Au regard de l'évolution de la structure des coûts, la part du budget de fonctionnement de la DSN consacré à la sécurité sera en augmentation dans les années à venir :

- En 2022, Autour de 3,9 % des effectifs de la DSN est consacré à la sécurité (19 UP).
- En 2025, la part des effectifs de la DSN consacrés à la sécurité passera à $\approx 5,0$ %

ANNEXE 3 : OBLIGATIONS LEGALES ET REGLEMENTAIRES

La mise en œuvre et l'utilisation des SN 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 des SN de l'AP-HP aux exigences légales et réglementaires**, en particulier :

- Le Règlement Général de Protection des données (RGPD)
- Le Règlement eIDAS relatif au moyen d'identification électronique.
- La Directive NETWORK AND INFORMATION SYSTEM SECURITY (NIS)
- Le Code la Santé Publique
- Le Code Pénal
- Le Code de la consommation
- Le Code de la propriété Intellectuelle
- La Loi Informatique et Libertés (LIL)
- 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'Etat et l'administration : le Référentiel Général de Sécurité (RGS)
- Les politiques de sécurité des SI émises par l'Etat (PSSI-E), le ministère des Solidarités et de la Santé (PSSI-S) et de l'ANS (Agence du Numérique en Santé),
- Loi république numérique
- Loi Hadopi
- Loi confiance dans l'économie numérique
- Loi relative aux recherches impliquant la personne humaine
- Loi modernisation du système de santé de 2016

L'AP-HP vise à se conformer à d'autres référentiels dont le MATURIN'H et le Programme SUN'ES.

L'AP-HP souhaite également se conformer aux exigences normatives décrites par les normes ISO27001, son annexe A et aux autres normes du référentiel HDS.

Pour les services HDS, un registre de la réglementation applicable est tenu à jour par la DSN.

ANNEXE 4 : INSTANCES DE PILOTAGE DE LA SECURITE

Comités dédiés à la sécurité des services numériques

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

Comités dédiés à la sécurité	Participants	Fréquence	Objectifs
Comité Stratégique de Sécurité de l'information	DGA Directeur de la DSN DSI GHU/Site/PIC RSSI GHU SORBONNE & SACLAY Directeurs de pôles et de programmes de la DSN Délégué Défense et Sécurité Directrice de la QPQAM RSSI et responsables de domaine du pôle DSN/SSI	Semestrielle	Etat d'avancement des actions décidées à l'issue du dernier COSTRAT Modifications des enjeux externes et internes pertinents en lien avec la sécurité de l'information Retours sur les performances de sécurité de l'information Gestion de crise cyber Retours d'information des parties intéressées Résultats de l'appréciation des risques et l'état d'avancement du plan de traitement des risques Opportunités d'amélioration continue
Réunion RSSI	RSSI AP-HP RSSI des GHU/Site/PIC	Mensuelle	Partager les informations relatives à la sécurité entre le RSSI de l'AP-HP et les RSSI des GHU et des sites
Comité de suivi de la sécurité	Directeur DSN RSSI AP-HP Pôles de la DSN	Trimestrielle	Suivre les projets, les incidents et piloter la sécurité par les risques
Revue de direction du SMSI	Directeur DSN Responsable SMSI Responsables des processus du SMSI HDS	Annuelle	Réaliser un bilan du cycle écoulé, présenter les indicateurs de performance et d'amélioration de la sécurité, présenter les opportunités d'amélioration.
Comité de revue des risques SI	Direction DSN RSSI AP-HP chargé de la gestion des risques SI Pilote Responsables et gestionnaire de risques SI	Semestriel	Etat d'avancement des actions décidées à l'issue du dernier comité de gestion des risques Résultats de l'appréciation des risques SI et l'état d'avancement du plan de traitement des risques Opportunités d'amélioration continue