

Politique Générale de Sécurité de l'Information (PGSI) de l'AP-HP

1.31

C0 – Public

En cours

Table des matières

1	LETRE D'ENGAGEMENT DE LA DIRECTION	3
2	INTRODUCTION	4
3	OBJECTIFS STRATEGIQUES DE SECURITE.....	7
4	ORGANISATION GENERALE DE LA SECURITE.....	7
5	CORPUS DOCUMENTAIRE	12
6	EXIGENCES DE SECURITE COMPLEMENTAIRES.....	13
	ANNEXE 1 : GLOSSAIRE DE LA SECURITE	16
	ANNEXE 2 : OBLIGATIONS LEGALES ET REGLEMENTAIRES	19
	ANNEXE 3 : INSTANCES DE PILOTAGE DE LA SECURITE.....	21
	ANNEXE 4 : INSTITUTIONS ET SITES DE REFERENCE	21

Référence	PO_AP-HP - PGSI V1.30.docx
Prochaine mise à jour	2026
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
1.21	22/04/2025	PERRET D.	Revue 2025
1.30	22/08/2025	PERRET D.	Intégration des évolutions réglementaires NIS V2, HDS V2, REC, IA-ACT. Retrait des références au SDSI 2020-2025.
1.31	01/10/2025	PERRET D	Validation par le DGA Monsieur Etienne GAYAT Directeur Général Adjoint de l'AP-HP

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 groupements hospitaliers universitaires (GHU) et leurs hôpitaux, ainsi que les pôles d'intérêt communs (PIC) de l'AP-HP. Pour y faire face, deux approches complémentaires doivent être menées.

Grands Principes de Sécurité Numérique

La disponibilité :

Les Services Numériques (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 :

Les 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 PGSI 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 des systèmes d'information.

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 (PGSSI-S).

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

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

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 Pôles d'Intérêt Commun (PIC), les hôpitaux non rattachés (HNR) 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 (RSSI) de l'AP-HP.

2.4 Cadre de référence

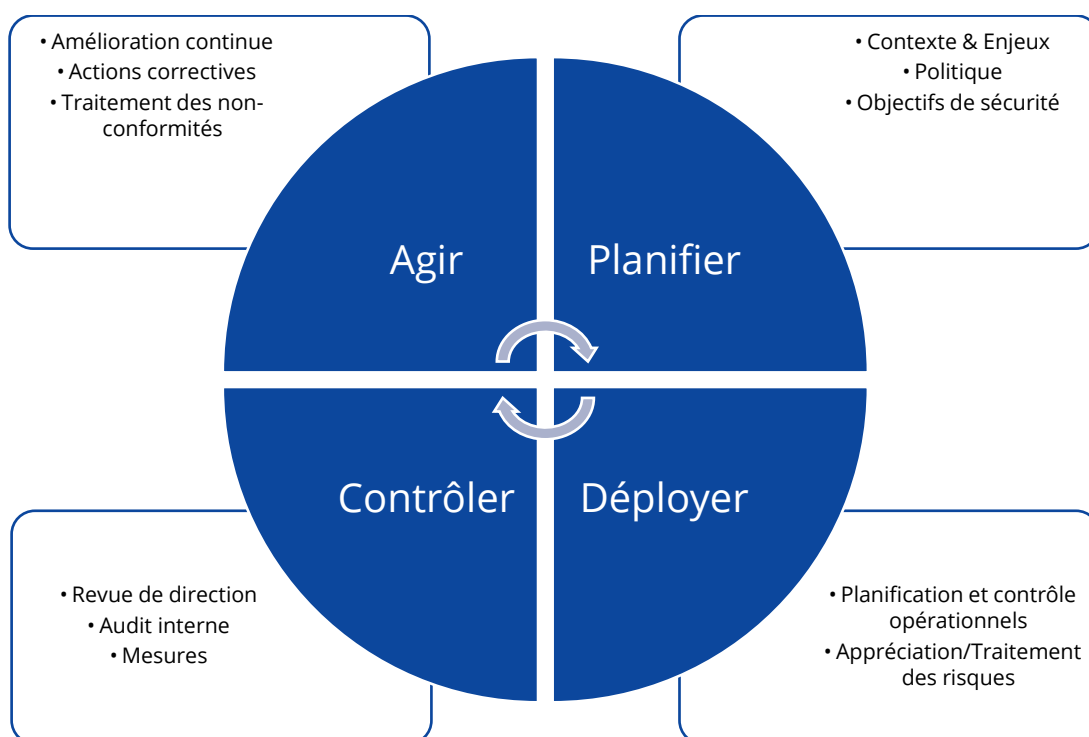
La Sécurité des SN de l'AP-HP est formalisée dans un référentiel documentaire dont la présente **Politique** constitue le premier niveau, fixant les principes de sécurité et les orientations d'organisation (Cf. CORPUS DOCUMENTAIRE CORPUS DOCUMENTAIRE à la page N°12 et suivantes).

Elle est complétée par **Charte informatique de l'AP-HP** annexe n°15 du **Règlement Intérieur** de l'AP-HP décrivant les règles d'usage du SI.

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 NF ISO/IEC 27001 version 2023**.

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 afin d'optimiser la gestion des risques, d'assurer l'efficacité opérationnelle, d'optimiser le ROI et de développer la confiance des parties.

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 et en homologuant la sécurité des services.

Gestion identités & accès

Maîtriser et sécuriser l'accès aux Services Numériques en conformité avec les exigences des référentiels nationaux et européens d'identités pour les patients et les professionnels.

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 graves de sécurité en assurant la continuité des activités informatiques et en adaptant l'organisation en cas de situation exceptionnelle.

Ces 8 objectifs stratégiques sont pilotés par des indicateurs revus en lors des comités de pilotage de la sécurité de l'information (COSTRAT CYBER, COPIL CYBER).

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 informatique de l'AP-HP** annexe n°15 du **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 marchés publics ou de conventions accédant aux SN de l'AP-HP ainsi qu'à tout opérateur économique intervenant pour leur compte, elles doivent être précisées dans le marché public 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 GHU, des PIC et HNR. 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 rapport 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 :

1. Gouvernance et pilotage

- Préparer et animer la gouvernance dédiée à la SSI en mobilisant les parties prenantes.
- Animer la filière sécurité SI et coordonner les RSSI des GHU, PIC et HNR.
- Diffuser et mettre à jour la PGSI, définir et piloter le plan d'audit.
- Piloter la mise en conformité du SI avec les règlements et directives européennes (NIS2, REC, CRA, RGPD, IA-ACT...).
- Rendre compte régulièrement à la Direction de la performance sécuritaire (SMSI inclus).
- Contribuer aux COPIL de la DSN, au schéma directeur des SN, et conseiller les entités.
- Représenter l'AP-HP dans les groupes externes de réflexion sur la cybersécurité.

2. Gestion des risques de sécurité de l'information et conformité

- Identifier, quantifier et traiter les risques de sécurité majeurs et transverses selon la méthode ISO 27005.
- Développer la démarche d'intégration de la sécurité dans les projets.
- Accompagner le DPO pour les AIPD, la revue des contrats et les audits de sous-traitants (CNIL).
- Assurer la fonction de référent informatique pour la certification des comptes.

3. Système de management de la sécurité (SMSI)

- Mettre en œuvre et améliorer le SMSI selon ISO/IEC 27001.
- Définir et suivre les indicateurs de performance de la sécurité permettant de piloter l'atteinte des objectifs de sécurité et la performance des processus de la DSN.
- Développer l'amélioration continue (revues, actions correctives, audits).

4. Prévention et sensibilisation

- Porter les projets transverses de sensibilisation et formation des utilisateurs à la sécurité de l'information.
- Assurer la veille sur les menaces.
- Mettre en œuvre, surveiller et améliorer les mesures de sécurité nécessaires au traitement des risques de sécurité de l'information et gérer les dispositifs de sécurité associés.
- Identifier et évaluer les solutions et les services de sécurité émergents.
- Assurer l'expertise technique et le support en matière de sécurité.

5. Gestion des incidents et continuité

- Préparer et piloter la gestion de crise cyber, en lien avec les directions qualité.
- Mettre en place et opérer les outils de détection et remédiation en temps réel (SOC).
- Assurer la gestion de la ligne d'astreinte cyber.
- Assurer la veille sécurité (menaces, vulnérabilités) en lien avec CERT-FR, CERT-Santé.

- Notifier les incidents de sécurité de l'information à l'ANSSI, l'ANS et à la CNIL par la DPO.
- Organiser l'accompagnement de la Direction générale et de ses représentants, ainsi que les Directions de GHU dans les chantiers de continuité et de reprise d'activité métier (PCRA) sur les périmètres relevant des technologies de l'information et de la communication.

6. Relations institutionnelles et ministérielles

- Piloter les programmes cyber définis par le ministère de la santé, l'ANSSI et l'ARS.
- Assurer la coordination et les comptes-rendus réglementaires auprès des autorités compétentes.

4.4.2 Les RSSI GHU/PIC/HNR

Les RSSI des GHU/PIC/HNR 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, des postes de travail, etc.), en priorisant ces mesures par rapport aux moyens dont ils disposent.

À ce titre, ils doivent notamment :

1. Gouvernance et pilotage

- Être les relais locaux du RSSI AP-HP.
- Assurer un rapport régulier sur la performance sécuritaire contribuant au système de management de la sécurité de l'information.
- Appuyer les contrôles du DPO et la mise en conformité NIS2.
- Animer la filière SSI sur son périmètre.
- Contribuer aux comités et audits internes locaux.

2. Gestion des risques de sécurité de l'information et conformité

- Tenir à jour la cartographie des risques locaux.
- Proposer les traitements et arbitrages.
- Intégrer la sécurité "by design" dans les projets locaux.
- Réaliser les revues d'architecture et l'homologation de sécurité pour les projets locaux.

3. Système de management de la sécurité (SMSI)

- 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 Services Numériques et les formaliser dans un plan d'actions chiffré, le communiquer au RSSI de l'AP.
- Appuyer au déploiement des solutions de sécurité (MFA, EDR, chiffrement, journalisation, bastions, segmentation, sauvegardes).
- S'assurer de l'activation et la bonne configuration des solutions de sécurité.
- Accompagner la lutte contre l'obsolescence et vulnérabilités (Inventaire des versions. Coordination du patch management. Traitement des actifs non supportés).
- Accompagner le décommissionnement et la fin de vie (Effacement des données. Révocation des accès. Mise au rebut sécurisée des supports/équipements).
- Exiger et contrôler les clauses et preuves de sécurité dans les contrats et conventions avec les fournisseurs.

4. Sensibilisation et accompagnement

- Organiser la sensibilisation SSI des équipes locales.
- Appuyer l'appropriation des règles et procédures.

5. Gestion des incidents de sécurité et continuité

- Coordonner la réponse locale aux incidents de sécurité.
- Assurer la notification interne auprès du RSSI.

- Contribuer à la préparation et aux tests la continuité des Technologies de l'Information et Communication (TIC) et la reprise d'activité pour les services critiques (PCRA).
- Contribuer aux exercices de crise.

6. Identités, habilitations et comptes à privilège

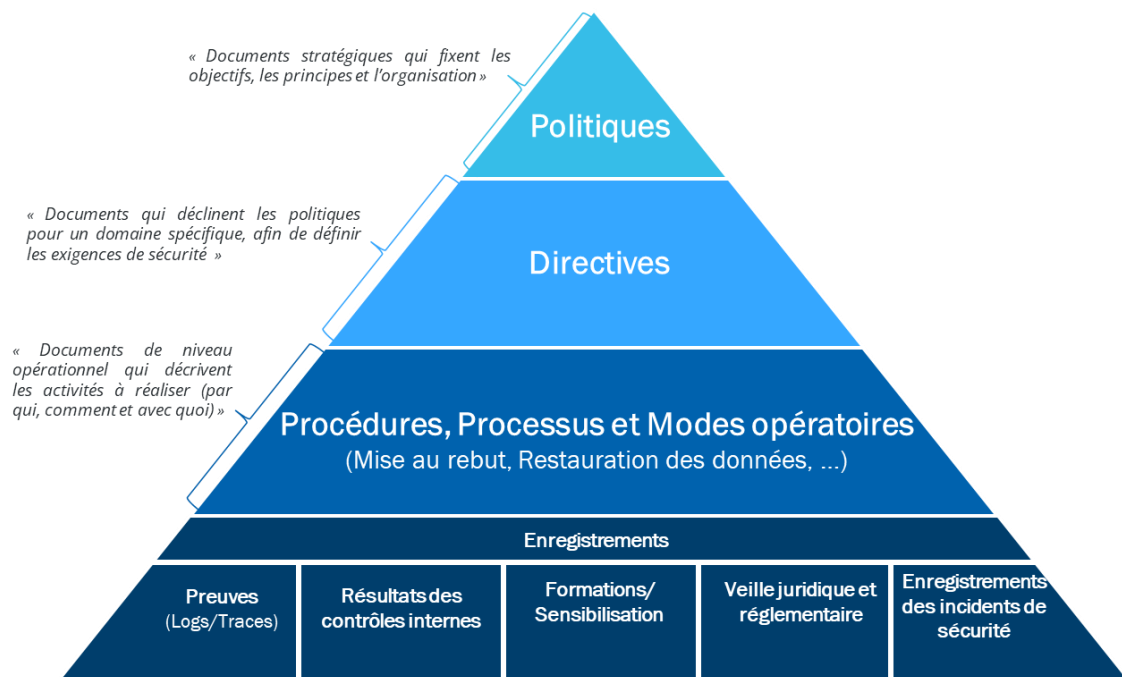
- Contribuer définir et valider les matrices d'habilitations (profils et droits associés), en conformité aux risques, aux enjeux et à la réglementation applicable.
- Superviser et contrôler les accès privilégiés (PAM, JIT/JEA).
- Effectuer un contrôle des habilitations du personnel des SN de son périmètre.
- Vérifier la réalisation des contrôles sur les habilitations des utilisateurs des SN par les responsables métiers.

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 « SERVICES NUMERIQUES » 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, maîtrise d'ouvrage, maîtrise d'œuvre, prestataires, acheteurs, personnels chargés de la mise en œuvre des services numériques... est regroupées dans un espace dédié accessible depuis [O6 SECURITE](#).

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 version 2023 :

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.

Les directives sont complétées par la procédure de gestion du système de management de la sécurité de l'information (SMSI), la procédure de gestion des risques de sécurité de l'information ainsi que les indicateurs de sécurité mesurant l'atteinte des objectifs de sécurité.

6 EXIGENCES DE SECURITE COMPLEMENTAIRES

Les attaques informatiques évoluent vite (Cf. ANSSI). Le secteur santé est ciblé (Cf. ENISA). Les exigences réglementaires en matière de sécurité se renforcent (Cf. EU). Le développement continu du numérique augmente la surface d'attaque de l'AP-HP (Cf. SDSI).

Ce chapitre formalise des exigences complémentaires qui devront être prises en compte au cours des 5 prochaines années pour maintenir un haut niveau de sécurité, la confiance des patients et des professionnels et limiter l'impact d'une attaque réussie.

Ces exigences assurent l'alignement avec la Directive NIS2, le référentiel HDS v2, SECNUMCLOUD, l'AI ACT et le Cyber RESILIENCE ACT, et font l'objet d'une veille avec une révision annuelle ou immédiate en cas de nouveau texte ou de menace critique.

Formation pour améliorer la performance des opérations de sécurité

Les menaces et les technologies de sécurité sont en constante évolution. Les personnels informatiques doivent se former pour adopter les bons réflexes en cas d'attaque informatique et adopter les meilleures pratiques de prévention au quotidien (sécurité par défaut et à la conception).

Authentification forte et résistante à l'hameçonnage

L'AP-HP impose l'authentification à plusieurs facteurs résistante à l'hameçonnage (FIDO2/WEBAUTHN ou équivalent PKI) pour tous les accès d'administration, les applications manipulant des données de santé, les VPN et la messagerie. Les méthodes OTP par SMS, courriel ou « PUSH » seules sont à proscrire.

Gouvernance de l'IA

Tout usage d'IA doit respecter le RGPD et le Règlement (UE) 2024/1689. Les projets doivent réaliser une analyse de risques, documenter les données, les modèles et les prompts, protéger les secrets et mettre en place des garde-fous contre l'empoisonnement et les injections de prompt. Les logs IA et la traçabilité doivent être conservés.

Cloud et souveraineté

Pour les traitements sensibles, l'AP-HP privilégie des services qualifiés SECNUMCLOUD v3.2 ou des contrôles équivalents. Les clés de chiffrement doivent être maîtrisées par l'AP-HP et, quand possible, le chiffrement côté client doit être utilisé. Les accès d'administration des CLOUD doivent suivre les exigences SECNUMCLOUD, notamment la séparation et l'authentification à plusieurs facteurs résistante à l'hameçonnage

Chaîne d'approvisionnement logicielle

Les fournisseurs doivent livrer une nomenclature logicielle (SBOM) signés et des attestations de provenance. L'AP-HP doit exiger des processus de correction rapides et des avis au format VULNERABILITY EXPLOITABILITY EXCHANGE (VEX). Les composants doivent être surveillés en continu et mis à jour selon un SLA fondé sur la criticité.

Durcissement des équipements en frontière de l'Internet (VPN/ADC/WAF)

Les passerelles exposées à Internet doivent être inventoriées, patchées en priorité et isolées. Après correctif, l'invalidation des sessions en cours doit être obligatoire. Toute vulnérabilité critique doit déclencher des mesures compensatoires et une analyse des traces.

Dispositifs biomédicaux et IoT

Les équipements médicaux et IoT doivent être segmentés, inventoriés, durcis et mis à jour via des fenêtres planifiées. Les accès distants des mainteneurs doivent être contrôlés et journalisés. Les achats doivent exiger des engagements cybersécurité et des délais de patch.

Sauvegardes résilientes face aux rançongiciels

Les sauvegardes doivent suivre la règle 3-2-1 avec au moins un stockage immuable/hors ligne, des tests annuels de restauration et une séparation stricte des comptes d'administration de sauvegarde.

Continuité d'activité et atténuation DDoS

Les services critiques doivent être protégés par des capacités DDOS de niveau réseau et applicatif avec bascule vers un centre d'épuration. Des tests de crise doivent valider les procédures, les contacts et les SLA. Les architectures doivent intégrer une mise à l'échelle.

Exercices et gestion de crise cyber

Des exercices de crise cyber pluriannuels doivent être planifiés, couvrant décisionnel, communication et technique. Les retours d'expérience doivent alimenter les plans de réponse et la cartographie des risques.

Administration sécurisée et Zéro TRUST

L'administration doit suivre un modèle Zéro TRUST : systèmes d'administration dédiés, MFA résistante à l'hameçonnage, bastions, séparation des rôles, inventaire des chemins d'accès, contrôle continu et évaluation périodique des droits. Les annuaires et PAM doivent appliquer les recommandations ANSSI.

Préparation à la cryptographie post-quantique

L'AP-HP doit établir une feuille de route pour la cryptographie post-quantique : inventaire crypto, mise à jour des bibliothèques, exigences d'agilité et essais contrôlés des standards NIST. Les systèmes à longue durée de vie doivent adopter des approches hybrides pendant la transition.

Sécurité des sessions et des jetons

Les sessions web et API sont liées au dispositif et au contexte (IP, client, attestation). Toute suspicion d'intrusion déclenche la révocation globale des jetons, l'invalidation des sessions persistantes et la rotation des secrets OAUTH/OIDC.

Journalisation et détection

La PGSI doit rendre obligatoire une politique de journalisation conforme aux guides ANSSI, avec horodatage synchronisé, centralisation, rétention adaptée et intégration SIEM/SOC. Un socle minimal d'événements doit être défini et contrôlé annuellement.

Veille vulnérabilités et intelligence des menaces

L'AP-HP doit s'abonner aux flux CERT-FR et EU VULNERABILITY DATABASE (EUVD). Un processus doit corréler les avis avec l'inventaire des actifs et doit fixer des délais de remédiation selon l'exposition et l'exploitation active (KEV).

Table 1 : TABLEAU DES JALONS RÉGLEMENTAIRES (2025-2028)

Mesure	Jalon principal	Échéance
AI ACT (UE 2024/1689)	Interdictions & littératie IA	02/02/2025
AI ACT (UE 2024/1689)	GPAI & gouvernance	02/08/2025
AI ACT (UE 2024/1689)	Application générale (hors art. 6(1))	02/08/2026
AI ACT (UE 2024/1689)	Art. 6(1) - classification haut risque	02/08/2027
Cyber RESILIENCE ACT (UE 2024/2847)	Obligations principales applicables	11/12/2027
Data ACT (UE 2023/2854)	Application du règlement	12/09/2025
Data ACT (UE 2023/2854)	Fin des frais de SWITCHING	12/01/2027

Politique Générale de Sécurité de l'Information (PGSI) de l'AP-HP

eIDAS 2 (UE 2024/1183)	WALLETS EUDI fournis par MS (IA ADOPT.)	28/11/2026
NIS2 (UE 2022/2555)	Transposition FR et décrets d'application	2025-2026
ENISA ETL 2024	Tests DDoS et continuité renforcés	Annuel

ANNEXE 1 : GLOSSAIRE DE LA SECURITE

ADC : APPLICATION DELIVERY CONTROLLER. Équipement réseau optimisant la livraison des applications.

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.

API : Interface de programmation (https://fr.wikipedia.org/wiki/Interface_de_programmation)

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.

DDOS : Attaque par déni de service distribué

(https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service)

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.

FIDO2 : FAST IDENTITY ONLINE 2 (https://fr.wikipedia.org/wiki/Alliance_FIDO)

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

HDS : Hébergeur de données de santé.

HNR : Hôpitaux non rattachés à un GHU.

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.

IoT : Internet des objets (https://fr.wikipedia.org/wiki/Internet_des_objets)

KEV : KNOWN EXPLOITED VULNERABILITIES

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

MFA : Authentification multi-facteurs.

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

OAuth : OPEN AUTHORIZATION (<https://en.wikipedia.org/wiki/OAuth>)

OIDC : OPENID CONNECT (https://fr.wikipedia.org/wiki/OpenID_Connect)

OTP : ONE-TIME PASSWORD

(https://fr.wikipedia.org/wiki/Mot_de_passe_%C3%A0_usage_unique)

PAM : Gestion des accès privilégiés

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

PKI : Infrastructure à clés publiques

(https://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publices)

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 : 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 événements cyber.

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.

SBOM : SOFTWARE BILL OF MATERIALS

(https://en.wikipedia.org/wiki/Software_supply_chain)

SLA : Accord / Contrat de niveau de service

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.).

SDSN : Schéma Directeur des Services Numériques

SIEM : SECURITY INFORMATION AND EVENT MANAGEMENT

(https://en.wikipedia.org/wiki/Security_information_and_event_management)

SMS : SHORT MESSAGE SERVICE (<https://en.wikipedia.org/wiki/SMS>)

SN : Service numérique

SOC : Centre des Opérations de Sécurité

SSN : Sécurité des Services Numériques

TIC : Technologie de l'Information et de la Communication

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.

VPN : Réseau privé virtuel

WAF : WEB APPLICATION FIREWALL (https://en.wikipedia.org/wiki/Web_application_firewall)

ANNEXE 2 : 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 :

- RÈGLEMENT (UE) 2023/2854 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données)
- Le Règlement (UE) 2016/679 Général de Protection des données (RGPD),
- Le Règlement (UE) 2023/2854 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données (DATA ACT).
- Le Règlement (UE) 2024/1689 Etablissant des règles harmonisées concernant l'intelligence artificielle (IA-ACT),
- Le Règlement (UE) 910/2014 et sa version révisée 2024/1183 relatif au moyen d'identification électronique (eIDAS),
- Le Règlement (UE) 2024/2847 Exigences de cybersécurité horizontales pour les produits comportant des éléments numériques (CRA)
- Le Règlement (UE) 2025/327 relatif à l'espace européen des données de santé,
- La Directive (UE) 2022/2557 relative à la résilience des entités critiques (REC),
- La Directive (UE) 2016/1148 relative aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (NIS VI) et sa version révisée 2022/2555 (NIS V2),
- Le Code la Santé Publique,
- Le Code de la sécurité sociale,
- Le Code Pénal,
- Le Code de la consommation,
- Le Code de la propriété Intellectuelle,
- La Loi Informatique et Libertés (LIL),
- La Loi république numérique,
- La Loi Hadopi,
- La Loi confiance dans l'économie numérique,
- La Loi relative aux recherches impliquant la personne humaine,
- La Loi modernisation du système de santé de 2016,
- La Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique
- Le Référentiel Général de Sécurité (RGS),
- Le Référentiel de certification Hébergeur de données de santé (HDS) en version 2.0,
- Les politiques de sécurité des SI émises par l'Etat (PSSI-E) et le ministère chargé de la Santé (PSSI-S),
- La norme NF ISO 27001 version 2023.

Les Règlements (UE) 2024/1689 (AI ACT) et le Règlement (UE) 2024/2847 (CRA) sont pris en compte pour les activités d'acquisition, d'intégration et de développement interne de produits et systèmes numériques, ainsi que pour la gouvernance des systèmes d'IA utilisés à des fins de soins, de recherche ou de gestion.

L'AP-HP vise à se conformer l'instruction N° DNS/2025/12 du 22 janvier 2025 relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires.

Politique Générale de Sécurité de l'Information (PGSI) de l'AP-HP

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 3 : INSTANCES DE PILOTAGE DE LA SECURITE

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

Nom	Objectifs	Organisation
COPIL CYBER ¹	Partager les actualités stratégiques sur la sécurité de l'information à l'AP-HP, notamment sur la base des indicateurs stratégiques CYBER. Revoir les priorités relatives des projets et activités récurrentes dans le domaine, et suivre l'avancement des plus prioritaires. Prendre des orientations et décisions, et préparer collaborativement des éventuelles propositions d'orientation pour la direction générale. Valider formellement le rapport annuel cyber.	Animation Présidence direction DGA/DSN, avec vice-présidence direction DQ2P. Secrétariat pôle SSI (invitation visioconférence, fixation ordre du jour en lien avec direction DSN et DQ2P, préparation collaborative du support, relevé de décision, gestion documentaire de l'historique, etc.). Régularité 1h tous les trimestres, à l'occasion d'un CODIR DSN élargi. Participants CODIR DSN Elargi, DQ2P, Sécurité générale.
COSUI CYBER	Partager les actualités opérationnelles sur la sécurité de l'information à l'AP-HP. Présenter l'avancement des projets et activités récurrentes sur lesquels un partage est pertinent dans une optique de coordination.	Animation Présidence pôle SSI. Secrétariat pôle RSSI (invitation visioconférence, fixation ordre du jour en lien avec GHU/PIC/HNR, préparation collaborative du support, relevé de décision, gestion documentaire de l'historique, etc.). Régularité 1h30 tous les mois. Participants RSSI de GHU/PIC/HNR et invités ponctuels en fonction des sujets.
Rapport annuel CYBER ²	Synthèse sur l'année en termes de CYBER, pour valoriser les réussites et mettre en lumière les difficultés, en prenant du recul. Mieux tracer nos politiques CYBER.	Rédigé par le pôle RSSI en décembre année N, pour circularisation du projet en janvier N+1 et séance de présentation au DG (et/ou point en CYBER DG en février N+1).
Indicateurs stratégiques CYBER	Support de pilotage pour le COPIL CYBER. Partage d'information transverse (hors informations sensibles).	Trimestriel dans le compte-rendu hebdomadaire DG.

Un COPIL CYBER résilience est organisé par le DQ2P chargé pilotage des plans de continuité et de reprise d'activités avec les métiers et les GHU/PIC/HNR.

ANNEXE 4 : INSTITUTIONS ET SITES DE REFERENCE

ANS (Agence du Numérique en Santé) : <https://esante.gouv.fr/>

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : <https://cyber.gouv.fr/>

CNIL (Commission Nationale de l'Informatique et des Libertés) : <https://www.cnil.fr/fr>

ENISA (Agence européenne pour la cybersécurité) : <https://www.enisa.europa.eu/>

ISO (Organisation internationale de normalisation) : <https://www.iso.org/home.html>

¹ Les éventuels points d'arbitrages complexes ou particulièrement stratégiques seront remontés, à l'issue de leur analyse par le COPIL Cyber, par le directeur de la DSN, le RSSI et la DQ2P pour inscription à l'ordre du jour Codir DG AP-HP, permettant notamment d'appuyer certains éléments auprès des directeurs des GHU/PIC.

² Doit inclure une section cyber-résilience, rédigée par la DQ2P.