|  |
| --- |
| CHU Ynov |
| Politique de Sécurité des Systèmes D’Information |
| Version 1.0 |

|  |
| --- |
| Xavier Martin  [Date] |

Table des matières

[1. Objet et finalité de la PSSI 5](#_Toc199840575)

[2. Portée de la politique 8](#_Toc199840576)

[2.1. Périmètre organisationnel : Identification fine des acteurs et des responsabilités 8](#_Toc199840577)

[2.2. Périmètre technique : Cartographie détaillée des actifs numériques et des infrastructures 10](#_Toc199840578)

[2.3. Périmètre informationnel : Classification, protection et gouvernance des données 12](#_Toc199840579)

[2.4. Périmètre temporel : Sécurisation sur l’ensemble du cycle de vie du système et des données 13](#_Toc199840580)

[2.5. Environnements couverts : Interopérabilité et gestion des interfaces 14](#_Toc199840581)

[2.6. Conformité réglementaire et normative : Cadre légal incontournable 15](#_Toc199840582)

[2.7. Limites et exclusions 15](#_Toc199840583)

[3. Cadre réglementaire et normatif 16](#_Toc199840584)

[3.1. Cadre juridique et réglementaire français 16](#_Toc199840585)

[3.2. Référentiels de l’Agence nationale de la sécurité des systèmes d’information (ANSSI) 16](#_Toc199840586)

[3.3. Normes et standards internationaux 17](#_Toc199840587)

[3.4. Contrats, certifications et engagements externes 18](#_Toc199840588)

[3.5. Audits, contrôles et régulation 18](#_Toc199840589)

[4. Objectifs de la politique 19](#_Toc199840590)

[4.1. Pilotage stratégique 19](#_Toc199840591)

[4.2. Responsabilités et rôles clés 20](#_Toc199840592)

[4.3. Intégration de la sécurité dans les projets 20](#_Toc199840593)

[4.4. Gestion des incidents et crises de cybersécurité 21](#_Toc199840594)

[4.5. Pilotage de la conformité, suivi et amélioration continue 21](#_Toc199840595)

[5. Gouvernance de la sécurité du SI 22](#_Toc199840596)

[5.1. Principes directeurs 22](#_Toc199840597)

[5.2. Méthodologie d’analyse des risques 22](#_Toc199840598)

[5.3. Cycles d’analyse périodique 24](#_Toc199840599)

[5.4. Responsabilités dans la gestion des risques 24](#_Toc199840600)

[5.5. Intégration dans la démarche globale de sécurité 24](#_Toc199840601)

[6. Classification et gestion des actifs 25](#_Toc199840602)

[6.1. Mesures organisationnelles 25](#_Toc199840603)

[6.2. Mesures techniques 26](#_Toc199840604)

[6.3. Mesures physiques 27](#_Toc199840605)

[7. Contrôle des accès et authentification 28](#_Toc199840606)

[7.1. Définition d’un incident de sécurité 28](#_Toc199840607)

[7.2. Processus de gestion des incidents 29](#_Toc199840608)

[7.3. Responsabilités et coordination 30](#_Toc199840609)

[7.4. Moyens techniques et logistiques 30](#_Toc199840610)

[7.5. Communication en situation de crise 30](#_Toc199840611)

[7.6. Suivi des incidents et indicateurs de performance 31](#_Toc199840612)

[8. Sécurité physique et environnementale 31](#_Toc199840613)

[8.1. Objectifs de la politique IAM 31](#_Toc199840614)

[8.2. Cycle de vie des identités 32](#_Toc199840615)

[8.3. Authentification et contrôles d’accès 33](#_Toc199840616)

[8.4. Revue et audit des habilitations 33](#_Toc199840617)

[8.5. Gestion des accès privilégiés (PAM – Privileged Access Management) 34](#_Toc199840618)

[8.6. Accès des prestataires et tiers 34](#_Toc199840619)

[8.7. Sensibilisation et formation 34](#_Toc199840620)

[8.8. Outils de support IAM 34](#_Toc199840621)

[9. Sécurité des communications et réseaux 35](#_Toc199840622)

[9.1. Objectifs stratégiques 35](#_Toc199840623)

[9.2. Politique de sauvegarde 35](#_Toc199840624)

[9.2.1. Typologie des données sauvegardées 35](#_Toc199840625)

[9.2.2. Principes de sauvegarde 35](#_Toc199840626)

[9.2.3. Outils et technologies 36](#_Toc199840627)

[9.3. Politique de continuité d’activité (PCA) 36](#_Toc199840628)

[9.3.1. Identification des processus critiques 36](#_Toc199840629)

[9.3.2. Mesures de continuité 36](#_Toc199840630)

[9.3.3. Maintenance du PCA 36](#_Toc199840631)

[9.4. Politique de reprise d’activité (PRA) 37](#_Toc199840632)

[9.4.1. Objectifs du PRA 37](#_Toc199840633)

[9.4.2. Plan de Reprise Informatique (PRI) 37](#_Toc199840634)

[9.4.3. Environnements de secours 37](#_Toc199840635)

[9.4.4. Reprise après cyberattaque 37](#_Toc199840636)

[9.5. Organisation et responsabilités 37](#_Toc199840637)

[9.6. Tests, audits et amélioration continue 38](#_Toc199840638)

[10. Sécurité des systèmes et applications 38](#_Toc199840639)

[10.1. Objectifs généraux 38](#_Toc199840640)

[10.2. Inventaire et classification 38](#_Toc199840641)

[10.3. Sécurisation à l’acquisition 39](#_Toc199840642)

[10.4. Intégration au réseau hospitalier 39](#_Toc199840643)

[10.5. Gestion des mises à jour et correctifs 39](#_Toc199840644)

[10.6. Authentification et accès 39](#_Toc199840645)

[10.7. Surveillance et supervision 40](#_Toc199840646)

[10.8. Fin de vie et décommissionnement 40](#_Toc199840647)

[10.9. Sensibilisation et collaboration 40](#_Toc199840648)

[11. Protection contre les logiciels malveillants 41](#_Toc199840649)

[11.1. Objectifs 41](#_Toc199840650)

[11.2. Périmètre de la journalisation 41](#_Toc199840651)

[11.3. Événements à journaliser 41](#_Toc199840652)

[11.4. Conditions de journalisation 42](#_Toc199840653)

[11.5. Centralisation et conservation 42](#_Toc199840654)

[11.6. Accès aux journaux 42](#_Toc199840655)

[11.7. Analyse et exploitation 43](#_Toc199840656)

[11.8. Formation et sensibilisation 43](#_Toc199840657)

[11.9. Évolutivité et conformité continue 43](#_Toc199840658)

[12. Gestion des incidents de sécurité 44](#_Toc199840659)

[12.1. Objectifs 44](#_Toc199840660)

[12.2. Intégration de la sécurité dans le cycle de vie des projets (SDLC) 44](#_Toc199840661)

[12.3. Gouvernance des projets SSI 44](#_Toc199840662)

[12.4. Documentation et traçabilité 45](#_Toc199840663)

[12.5. Projets externalisés ou SaaS 45](#_Toc199840664)

[12.6. Évaluation continue 45](#_Toc199840665)

[13. Continuité d’activité et reprise après sinistre 45](#_Toc199840666)

[13.1. Objectifs 45](#_Toc199840667)

[13.2. Publics cibles 46](#_Toc199840668)

[13.3. Contenus pédagogiques et thématiques abordées 46](#_Toc199840669)

[13.4. Moyens pédagogiques 47](#_Toc199840670)

[13.5. Suivi, évaluation et amélioration 47](#_Toc199840671)

[13.6. Responsabilités 47](#_Toc199840672)

[14. Sensibilisation et formation des utilisateurs 48](#_Toc199840673)

[14.1. Objectifs 48](#_Toc199840674)

[14.2. Typologie des tiers concernés 48](#_Toc199840675)

[14.3. Exigences contractuelles de sécurité 49](#_Toc199840676)

[14.4. Processus d’intégration et de suivi des tiers 49](#_Toc199840677)

[14.5. Responsabilités 49](#_Toc199840678)

[14.6. Mesures spécifiques en cas de sous-traitance 49](#_Toc199840679)

[15. Sécurité des prestataires et des tiers 50](#_Toc199840680)

[15.1. Objectif 50](#_Toc199840681)

[15.2. Définition de la situation de crise SI 50](#_Toc199840682)

[15.3. Préparation et anticipation 50](#_Toc199840683)

[15.4. Organisation de la gestion de crise 51](#_Toc199840684)

[15.5. Outils et ressources dédiés 51](#_Toc199840685)

[15.6. Reprise d’activité et retour à la normale 51](#_Toc199840686)

[15.7. Responsabilités 51](#_Toc199840687)

[15.8. Amélioration continue 52](#_Toc199840688)

[16. Conformité, audit et amélioration continue 52](#_Toc199840689)

[16.1. Objectifs 52](#_Toc199840690)

[16.2. Dispositif de surveillance 52](#_Toc199840691)

[16.3. Audit de sécurité 53](#_Toc199840692)

[16.4. Contrôles internes 53](#_Toc199840693)

[16.5. Responsabilités 53](#_Toc199840694)

[16.6. Amélioration continue 54](#_Toc199840695)

[17. Annexe – Documents de référence 54](#_Toc199840696)

[17.1. Documents internes 54](#_Toc199840697)

[17.2. Référentiels et normes externes 55](#_Toc199840698)

[17.3. Cadres contractuels 55](#_Toc199840699)

[17.4. Maintenance et diffusion des annexes 55](#_Toc199840700)

[18. Entrée en vigueur 56](#_Toc199840701)

# 1. Objet et finalité de la PSSI

La Politique de Sécurité des Systèmes d’Information (PSSI) du CHU YNOV est le document de référence qui explicite l’engagement institutionnel, stratégique et opérationnel de l’établissement en matière de cybersécurité. Elle a pour objectif de garantir la protection, la résilience, l'intégrité, la confidentialité et la disponibilité des ressources numériques du CHU, considérées comme essentielles à la mission de santé publique et à la continuité des soins.

Cette politique s’inscrit dans une logique de gouvernance globale du système d’information hospitalier (SIH), en intégrant la sécurité comme un axe transverse, structurant et piloté, en cohérence avec les ambitions de modernisation numérique de l’établissement. Elle repose sur une démarche proactive de gestion des risques, s’appuyant à la fois sur des exigences réglementaires, des normes reconnues, des bonnes pratiques sectorielles et une culture de responsabilité partagée.

La PSSI concerne et engage l’ensemble des parties prenantes du CHU YNOV : personnels médicaux, paramédicaux, administratifs, techniques, informaticiens, chercheurs, étudiants, prestataires, sous-traitants, partenaires institutionnels ou industriels. Elle s’impose également à toute entité ou individu ayant un accès aux systèmes d’information ou manipulant des données produites, hébergées ou traitées par l’établissement.

Enjeux stratégiques et métiers couverts :

Soutien aux missions hospitalières : permettre le fonctionnement fiable, sécurisé et sans interruption des processus critiques liés à la prise en charge des patients, à l’activité médicale, à la recherche, à l’enseignement et à la gestion administrative.

Protection du patrimoine informationnel : préserver la confidentialité, l’intégrité et la disponibilité des données de santé, des informations cliniques, des dossiers patients, des résultats biologiques et des comptes-rendus médicaux, en conformité avec les exigences du RGPD, de la CNIL, du Code de la santé publique et de l’ANS.

Renforcement de la résilience cyber : faire face à l’évolution rapide et complexe des menaces informatiques (ransomwares, fuites de données, espionnage, sabotage, attaques internes), en dotant l’établissement d’une capacité robuste de prévention, de détection, de réponse et de remédiation.

Conformité réglementaire : répondre aux obligations imposées par les textes légaux et réglementaires français et européens (PGSSI-S, référentiel HOP’EN, MSSanté, instruction DGS, certification ISO 27001, décret hébergement HDS, PIA, plan national cybersécurité santé, etc.).

Mise en sécurité des projets numériques : assurer une intégration systématique de la sécurité dans le cycle de vie des projets (démarche "Security by Design"), de la conception à la mise en production, en passant par la contractualisation avec les fournisseurs et l’évaluation des impacts sur la vie privée (PIA).

Sensibilisation des acteurs : ancrer une culture partagée de la cybersécurité et de la gestion des risques numériques, en formant les utilisateurs à leurs responsabilités et aux bons comportements à adopter face aux menaces (phishing, fuite d’information, manipulation sociale, usage des mots de passe, etc.).

Objectifs fonctionnels et techniques de la PSSI :

Définir les principes directeurs, les responsabilités, les procédures et les moyens associés à la sécurité du SI.

Structurer la gouvernance de la sécurité autour d’un Responsable de la Sécurité des Systèmes d’Information (RSSI), de comités de pilotage, d’un plan de communication, de tableaux de bord de suivi et d’indicateurs.

Fournir un cadre opérationnel commun à toutes les initiatives de sécurité (audit, supervision, gestion des identités, cryptographie, journalisation, sauvegarde, gestion de crise, etc.).

Identifier, évaluer et traiter les risques SSI de manière dynamique, en cohérence avec les cartographies métiers, les plans de continuité (PCA/PRA) et les référentiels d’analyse de risque (EBIOS RM, MEHARI).

Favoriser la mutualisation des ressources de sécurité au sein du GHT AP-HM et l’interopérabilité sécurisée avec les autres établissements de santé, partenaires de recherche, laboratoires, applications en cloud santé, etc.

Portée prospective et d’innovation :

La PSSI soutient activement la transformation numérique de l’hôpital et la mise en œuvre de nouveaux usages numériques sécurisés, tels que :

* La télémédecine (téléconsultation, télé-expertise, télésurveillance),
* L’usage de dispositifs médicaux connectés (IoMT),
* L’intelligence artificielle appliquée au diagnostic et à l’aide à la décision,
* L’intégration de données massives (Big Data) dans les plateformes de recherche et d’enseignement,
* L’hébergement sécurisé des données de santé dans des infrastructures certifiées HDS.

Engagement dans l’amélioration continue :

La PSSI est révisée annuellement ou à l’occasion de tout changement majeur (incident critique, évolution du SI, modification réglementaire, fusion institutionnelle, etc.).

Elle est complétée par des politiques et procédures spécifiques : gestion des habilitations,charte utilisateur, politique de sauvegarde, plan de continuité informatique, politique de journalisation, etc.

Son efficacité est évaluée à travers des audits réguliers, des contrôles internes, des tests de sécurité (scans, pentests), des exercices de crise et des retours d’expérience (REX).

# 2. Portée de la politique

La portée de la Politique de Sécurité des Systèmes d’Information (PSSI) du CHU de La Timone est conçue pour couvrir de manière exhaustive tous les aspects liés à la sécurité, à la confidentialité, à l’intégrité, à la disponibilité et à la traçabilité des informations et des systèmes numériques, tout en s’inscrivant dans une dynamique d’adaptation permanente face à l’évolution des risques, des technologies et des cadres réglementaires.

Cette portée est multidimensionnelle et repose sur une cartographie précise des ressources, des processus métiers, des acteurs impliqués, des technologies employées et des environnements internes et externes. Elle permet de garantir que toutes les actions de sécurisation du SI sont cohérentes, harmonisées, et que les responsabilités sont clairement attribuées.

## 2.1. Périmètre organisationnel : Identification fine des acteurs et des responsabilités

La sécurité est une responsabilité partagée qui implique un large éventail d’acteurs internes et externes, avec des rôles, des droits et des obligations variés. La PSSI définit précisément ce périmètre humain et organisationnel, afin d’assurer un pilotage rigoureux et une sensibilisation adaptée :

**Personnel médical et paramédical**

Les utilisateurs directs des systèmes cliniques (dossiers patients, prescriptions, résultats d’examens)

Responsabilisés à travers des chartes d’utilisation, formation continue, procédures d’habilitation strictes

Interdiction de divulgation non autorisée, gestion rigoureuse des accès, obligations de confidentialité renforcées

Particularité : besoins spécifiques liés aux impératifs de soin en urgence et à la mobilité (usage d’appareils mobiles sécurisés, accès délégués, etc.)

**Personnel administratif et gestionnaire**

Gestionnaires des ressources humaines, finances, approvisionnements, juridique

Responsables de la gestion des contrats, facturations, données sensibles sur les patients et collaborateurs

Soumis à des contrôles d’accès granulaire, auditabilité et traçabilités accrues

**Équipes informatiques, cybersécurité et support technique**

Administration des infrastructures, développement, supervision et remédiation des incidents

Gestion des accès privilégiés (compte administrateur, comptes service), séparation des rôles et des privilèges

Mise en œuvre des politiques de sauvegarde, monitoring, gestion des vulnérabilités, gestion des incidents de sécurité

Implication dans la gouvernance SSI, reporting et amélioration continue

**Chercheurs, enseignants, étudiants**

Accès aux bases de données de recherche, plateformes collaboratives et outils d’analyse avancés

Sensibilisation spécifique aux enjeux de confidentialité, protection des résultats de recherche, respect des accords éthiques et réglementaires

Gestion adaptée des droits d’accès en fonction du rôle, de la nature des projets, du type de données manipulées

**Prestataires et fournisseurs externes**

Intégration sécurisée via des clauses contractuelles précises (NDA, engagements RGPD, plan de continuité d’activité)

Contrôle des accès via des comptes dédiés, gestion de la sous-traitance selon la réglementation en vigueur

Vérification régulière des dispositifs de sécurité des tiers, audits et évaluations périodiques

**Instances de gouvernance**

Direction générale, comité de pilotage SI, comité sécurité, délégué à la protection des données (DPO)

Responsables de la validation, du pilotage stratégique et opérationnel, de la coordination des actions de sécurité

Supervision des audits, gestion des incidents majeurs, arbitrages des ressources

**Utilisateurs mobiles et télétravailleurs**

Accès sécurisé via VPN, authentification multifactorielle (MFA), dispositifs cryptés

Application de politiques spécifiques pour la protection des terminaux BYOD (Bring Your Own Device)

Surveillance renforcée des connexions distantes, gestion des risques liés aux environnements hors contrôle physique du CHU

## 2.2. Périmètre technique : Cartographie détaillée des actifs numériques et des infrastructures

La PSSI englobe l’ensemble des composants du système d’information (SI) hospitalier, couvrant les couches physiques, logicielles, réseaux et services, afin d’assurer une protection cohérente et intégrée :

**Infrastructures physiques**

Centres de données internes, salles serveurs avec contrôle d’accès biométrique, vidéosurveillance, systèmes de détection d’intrusion physiques

Systèmes d’alimentation électrique redondante (UPS, groupes électrogènes), contrôle climatique, anti-incendie

Gestion des équipements réseaux, serveurs, postes de travail, terminaux mobiles

**Équipements réseau et sécurité**

Pare-feu nouvelle génération (NGFW), systèmes de détection/prévention d’intrusions (IDS/IPS)

Segmentation réseau rigoureuse : isolement des environnements production, développement, test, zones sensibles

Réseaux Wi-Fi sécurisés avec authentification forte (802.1X), usage de VLAN, chiffrement avancé (WPA3)

Mise en place de VPN pour accès distants sécurisés avec authentification multifactorielle

**Systèmes d’exploitation et plateformes applicatives**

Gestion des correctifs réguliers, configuration sécurisée selon les standards (benchmarks CIS, recommandations ANSSI)

Applications hospitalières critiques (SIH, DPI, PACS, systèmes de gestion de laboratoire) avec contrôles d’accès renforcés, traçabilité des actions

Solutions cloud (SaaS, IaaS, PaaS) certifiées HDS et conformes RGPD, intégrées selon un modèle d’hybridation sécurisé

Outils collaboratifs, messagerie sécurisée, solutions de téléconsultation avec chiffrement des échanges

**Objets connectés médicaux (IoMT)**

Dispositifs médicaux connectés intégrés dans un réseau sécurisé avec supervision continue

Mise à jour des firmwares et logiciels, contrôles d’intégrité, cryptographie des communications

Gestion des incidents de sécurité spécifiques liés à l’IoMT, plans de contingence

**Sécurité des postes de travail et mobiles**

Solutions antivirus/antimalware à jour, gestion centralisée des correctifs

Gestion des droits utilisateurs avec principe du moindre privilège

Mise en place d’outils de chiffrement des données stockées, verrouillage automatique, gestion des périphériques amovibles

Utilisation de solutions MDM/UEM pour gérer les terminaux mobiles et BYOD

**Mécanismes de sécurité transverses**

Authentification forte (MFA), gestion centralisée des identités et des accès (IAM), gestion des habilitations avec revues périodiques

Journalisation exhaustive et sécurisée des événements (logs), intégration dans un SIEM pour détection et corrélation des incidents

Sauvegardes régulières, plans de continuité (PCA) et reprise d’activité (PRA) testés et validés périodiquement

Politique de gestion des vulnérabilités, audits de sécurité réguliers, tests d’intrusion et analyses de risques dynamiques

## 2.3. Périmètre informationnel : Classification, protection et gouvernance des données

La PSSI couvre toutes les données manipulées au sein du CHU, avec une attention particulière sur la gestion différenciée selon la sensibilité, la criticité et la nature des informations :

**Données de santé personnelles (DCP)**

Protection renforcée conformément au RGPD, CNIL, Code de la santé publique

Mise en place de mesures techniques (chiffrement au repos et en transit, pseudonymisation, anonymisation)

Contrôle strict des accès, traçabilité et auditabilité des consultations et modifications

Gestion des consentements des patients, droits d’accès, portabilité et effacement

**Données administratives et RH**

Protection des données personnelles du personnel, conformité au Code du travail et à la réglementation sur la vie privée

Sécurisation des données sensibles (contrats, dossiers disciplinaires), gestion rigoureuse des habilitations

**Données financières et comptables**

Gestion sécurisée des flux financiers, données sensibles des partenaires, respect des exigences SOX, PCI DSS si applicables

**Données de recherche et innovation**

Respect des engagements éthiques, protocoles de confidentialité, sécurisation des bases de données collaboratives

Gestion des droits d’accès multi-niveaux selon les projets et les partenaires

**Données opérationnelles et logs**

Conservation sécurisée des traces, analyses comportementales, protection contre les accès non autorisés

Archivage conforme aux obligations légales, avec accès restreint

**Documents stratégiques et contractuels**

Politique de classification documentaire, gestion des accès et diffusion selon les niveaux de confidentialité

Protection juridique et conformité avec les normes de gouvernance

## 2.4. Périmètre temporel : Sécurisation sur l’ensemble du cycle de vie du système et des données

La politique s’applique tout au long du cycle de vie des actifs et des données, de leur création à leur destruction :

**Phase de conception et acquisition**

Intégration systématique de la sécurité dans les cahiers des charges et les appels d’offres (Security by Design)

Analyse d’impact relative à la protection des données (PIA) obligatoire pour tout projet impliquant des données sensibles

**Phase d’exploitation**

Mise en œuvre des contrôles d’accès, supervision en temps réel, gestion des incidents et réponse rapide

Formation continue des utilisateurs, gestion des mises à jour et correctifs

**Phase de maintenance**

Contrôles périodiques, audits de conformité, revues de droits et habilitations, tests de vulnérabilité

**Phase de décommissionnement et destruction**

Procédures sécurisées pour la destruction physique et logique des supports et données, certification de destruction

Archivage légal des données nécessaires selon les durées réglementaires

## 2.5. Environnements couverts : Interopérabilité et gestion des interfaces

La PSSI prend en compte l’ensemble des environnements connectés au SI, internes ou externes, afin d’éviter les risques liés aux interfaces et échanges inter-systèmes :

**Réseaux internes et périmètres locaux**

Segmentation fonctionnelle et physique, limitation des flux réseau selon le principe du besoin d’accès

Mise en place de DMZ pour isoler les services exposés

**Interopérabilité avec les partenaires de santé**

Conformité aux normes d’échange sécurisées (MSSanté, HPRIM, IHE)

Contrats et conventions précisant les responsabilités en matière de sécurité

**Intégration avec les plateformes cloud**

Analyse des risques spécifiques liés au cloud public, privé ou hybride

Mise en œuvre des garanties contractuelles et techniques (certifications, chiffrement, audit)

**Connexion aux réseaux mobiles et IoT**

Gestion renforcée des accès, surveillance des flux, protections spécifiques aux équipements mobiles

## 2.6. Conformité réglementaire et normative : Cadre légal incontournable

La PSSI est explicitement alignée avec les exigences légales nationales, européennes et internationales, notamment :

* RGPD et loi Informatique et Libertés : gestion des données personnelles et respect des droits des personnes
* Code de la santé publique : règles spécifiques applicables aux données de santé
* Certification HDS : exigences pour l’hébergement sécurisé des données de santé
* Référentiels ANSSI (PGSSI-S, EBIOS RM) : bonnes pratiques et méthodes d’analyse de risque
* Normes ISO 27001, ISO 27799 : cadre international pour le management de la sécurité et la protection des données de santé
* Textes spécifiques liés à la santé et au numérique (HOP’EN, MSSanté, plans nationaux cybersécurité santé)

## 2.7. Limites et exclusions

Pour garantir une clarté parfaite, la PSSI précise également ce qui ne relève pas de son périmètre, par exemple :

* Équipements personnels non autorisés (hors BYOD contrôlé)
* Services tiers non contractuels ou non validés par la direction SI
* Données ou systèmes hors du contrôle ou de la propriété du CHU, sauf dispositions contractuelles spécifiques

# 3. Cadre réglementaire et normatif

Le CHU YNOV opère dans un environnement fortement encadré par des exigences légales, réglementaires et normatives en matière de sécurité des systèmes d'information. La présente PSSI s’inscrit dans le respect strict de ces exigences, qu’elles soient issues de textes européens, nationaux ou de référentiels de bonnes pratiques reconnus au niveau international. L’objectif de ce cadre est d’assurer la conformité juridique, la protection des droits des usagers et la sécurisation des actifs critiques.

## 3.1. Cadre juridique et réglementaire français

Loi n°78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés : encadre la protection des données personnelles.

Règlement Général sur la Protection des Données (RGPD - UE 2016/679) : impose des obligations en matière de traitements des données à caractère personnel, d’information, de consentement, de droits des personnes et de notification de violation de données.

Code de la santé publique (CSP) : articles relatifs à la protection des données médicales, à l’hébergement agréé HDS (articles L1111-8 et suivants) et au dossier médical partagé (DMP).

Loi n°2004-575 pour la confiance dans l’économie numérique (LCEN) : concerne les responsabilités en matière de contenu, d’accès à Internet et de sécurité des réseaux.

Loi de programmation militaire (LPM) et décrets de sécurité relatifs aux opérateurs de services essentiels (OSE) : certains services du CHU peuvent relever de cette classification et être soumis à des exigences accrues.

Code du travail : inclut des obligations concernant la sécurité informatique et la protection des données dans le cadre professionnel.

## 3.2. Référentiels de l’Agence nationale de la sécurité des systèmes d’information (ANSSI)

Le CHU s’engage à appliquer les recommandations de l’ANSSI, notamment :

PGSSI-S (Politique Générale de Sécurité des Systèmes d’Information de Santé) : cadre de référence pour l’ensemble des établissements de santé en France.

Référentiel d’homologation de sécurité pour les services numériques sensibles.

Guide d’hygiène informatique (version 2022) : recueil des mesures de base à mettre en œuvre.

Référentiels techniques de cybersécurité (gestion des habilitations, segmentation réseau, supervision, durcissement des systèmes, gestion des vulnérabilités, PRA/PCA, etc.).

Politique de sécurité applicable aux systèmes d'information d'importance vitale (SIIV), si applicable.

## 3.3. Normes et standards internationaux

ISO/IEC 27001 : système de management de la sécurité de l’information (SMSI), base de la structure de gouvernance SSI.

ISO/IEC 27002 : guide des mesures de sécurité à mettre en œuvre pour chaque domaine (contrôle d’accès, cryptographie, sécurité physique, journalisation, etc.).

ISO/IEC 27005 : gestion des risques liés à la sécurité de l’information.

ISO/IEC 27701 : extension de la norme ISO 27001 pour le management de la protection des données à caractère personnel.

ISO 22301 : management de la continuité d’activité, complémentaire aux stratégies de PRA/PCA.

ISO/IEC 20000 : gestion des services IT intégrant les dimensions de sécurité.

NIST Cybersecurity Framework (CSF) : référentiel structurant autour des fonctions Identifier, Protéger, Détecter, Répondre, et Rétablir.

NIS2 : La directive NIS 2 (en français : sécurité des réseaux et des systèmes d'Information) vise à renforcer le niveau de cybersécurité des tissus économique et administratif des pays membres de l'UE.

L'enjeu est de mieux protéger les réseaux et les systèmes d'information servant à fournir des services essentiels dans les secteurs clés de nos sociétés. Alors que la première directive NIS visait à protéger les acteurs économiques majeurs de l'UE, cette nouvelle directive élargit le champ des entités et secteurs concernés et introduit des exigences plus adaptées, notamment au regard du renforcement de la menace cyber. Elle prévoit un socle de mesures juridiques, techniques et organisationnelles que les futures entités régulées devront mettre en œuvre, en fonction du risque existant, afin d'élever leur niveau général de cybersécurité et d'accroître leur résilience opérationnelle.

## 3.4. Contrats, certifications et engagements externes

Intégration systématique de clauses de sécurité dans les contrats de prestations et d’achats informatiques.

Suivi des prestataires certifiés HDS (hébergeurs de données de santé) selon les exigences de l’ASIP Santé.

Partenariats inter-hospitaliers (GHT, réseaux de soins, structures de recherche) assortis de chartes de sécurité ou de protocoles d’échange sécurisés.

Conformité aux exigences imposées par les appels d’offres publics (notamment les marchés RESAH et UGAP en matière de sécurité).

## 3.5. Audits, contrôles et régulation

Audits internes réguliers pour vérifier la conformité avec la présente PSSI, incluant les audits techniques, organisationnels et applicatifs.

Contrôles périodiques par la CNIL, notamment en cas de traitement massif de données de santé ou d’incidents de sécurité majeurs.

Surveillance par l’ARS (Agence Régionale de Santé) dans le cadre de la gouvernance numérique et de la cybersécurité.

Inspections de l’ANSSI ou du CERT Santé en cas d’incident majeur ou d’inscription dans un plan national (ex. Plan Cyber Résilience).

Évaluation de maturité SSI selon les référentiels nationaux (ex. grille de maturité PGSSI-S, indicateurs MSSanté, programme SUN-ES).

# 4. Objectifs de la politique

La gouvernance de la sécurité des systèmes d’information au sein du CHU de La Timone repose sur une organisation rigoureuse, pluridisciplinaire et proactive, articulée autour de principes directeurs visant à aligner la stratégie de cybersécurité avec les missions hospitalières, la qualité des soins, la protection des données de santé, et la continuité d’activité. Elle mobilise des acteurs institutionnels, techniques, administratifs et médicaux autour d’une vision commune de la sécurité numérique.

## 4.1. Pilotage stratégique

Le pilotage stratégique est placé sous l’autorité de la Direction Générale, garantissant l’engagement de la gouvernance au plus haut niveau. Cette approche est formalisée à travers plusieurs instances :

* Le Comité de Pilotage du Système d’Information (CPSI) : organe de gouvernance SI stratégique intégrant les enjeux de cybersécurité. Il approuve la PSSI, fixe les priorités en matière de sécurité, arbitre les moyens humains, financiers et techniques, et assure le suivi des plans d’actions SSI.
* Le Comité de Sécurité des Systèmes d’Information (CSSI) : comité technique et opérationnel coordonné par le RSSI, ayant pour mission de piloter la mise en œuvre de la PSSI, de suivre les indicateurs de sécurité, de traiter les incidents, et d’animer les démarches de sensibilisation et de conformité réglementaire.
* La Cellule de Crise SSI : activée en cas d’incident majeur, elle regroupe les fonctions essentielles (Direction, DSI, RSSI, DPO, Direction médicale, Communication, Juridique) pour coordonner la réponse aux incidents critiques.

## 4.2. Responsabilités et rôles clés

La répartition claire des responsabilités est un pilier fondamental de la gouvernance SSI. Les rôles essentiels sont définis comme suit :

* RSSI : rattaché à la Direction Générale ou à la DSI selon les modalités internes, il élabore, pilote et met à jour la PSSI, anime le CSSI, conseille la direction sur les risques cyber, coordonne les audits et supervise la gestion des incidents. Il propose les mesures de sécurité à mettre en œuvre et veille à leur conformité avec les référentiels (PGSSI-S, ISO 27001, NIS2…).
* DSI : en lien direct avec le RSSI, elle veille à l’implémentation technique des mesures de sécurité, à l’urbanisation cohérente du SI, à la maîtrise des architectures et à la sécurité opérationnelle des infrastructures, systèmes et réseaux.
* DPO : expert RGPD, il intervient dans toutes les décisions touchant aux données à caractère personnel. Il valide les analyses d’impact (AIPD), contrôle la conformité des traitements et participe à la gestion des violations de données personnelles.
* DRH : intégration de la cybersécurité dans le cycle de vie RH : contrats, clauses, parcours d’intégration, formations obligatoires, revues d’habilitations, sanctions disciplinaires en cas de compromission volontaire ou négligente.

Chefs de pôles, cadres de santé, responsables de services cliniques et médico-techniques : relais essentiels pour l’application de la PSSI au sein des unités de soin et laboratoires. Ils veillent à la sensibilisation des personnels, au respect des règles d’habilitation et à la remontée des incidents.

Utilisateurs finaux (soignants, administratifs, chercheurs, prestataires, stagiaires) : chacun est responsable de l’usage qu’il fait du SI. Leur comportement est encadré par la charte utilisateur SSI.

## 4.3. Intégration de la sécurité dans les projets

La gouvernance impose l’intégration systématique de la sécurité dans tous les projets :

Analyse de risques SSI projet (EBIOS RM ou méthode équivalente) obligatoire dès la phase d’étude.

Revues de sécurité en jalons : validation des architectures, des contrats (clauses SSI), des choix de solutions (homologuées, hébergement HDS, compatibilité avec référentiels ANS).

Homologation des nouveaux services : formalisation d’une autorisation de mise en production par le RSSI après vérification des contrôles de sécurité.

## 4.4. Gestion des incidents et crises de cybersécurité

Une gouvernance efficace s’appuie sur une capacité à réagir rapidement et efficacement :

Dispositif de détection avancé : supervision temps réel des événements de sécurité, SOC, outils d’analyse de logs, corrélation, EDR.

Procédures d’escalade : hiérarchisation des incidents (faible, moyen, critique), déclenchement d’astreinte SSI et activation du PCA/PRA.

Lien avec l’ANS, le CERT Santé, l’ARS, la CNIL : notifications obligatoires en cas d’incident significatif (ransomware, violation de données, interruption de soins).

Rétroanalyse et post-mortem : chaque incident majeur donne lieu à une revue complète, avec plan d’actions correctives documenté et suivi par le CSSI.

## 4.5. Pilotage de la conformité, suivi et amélioration continue

La gouvernance s’inscrit dans un cycle de progrès constant :

* Indicateurs SSI (KPI/KRI) : suivi de la conformité aux politiques, de l’exposition aux vulnérabilités, du taux de formation, de l’activité des dispositifs de sécurité.
* Audits de conformité : internes (auto-évaluations), croisés avec d’autres CHU, externes (HDS, ISO 27001), ou par des autorités (ARS, ANS, Cour des Comptes).
* Mécanisme de revue annuelle : analyse du retour d’expérience, bilan des incidents, évaluation des risques émergents, priorisation des mesures à intégrer dans le plan SSI annuel.
* Mise à jour de la PSSI : formalisée par le CSSI, validée par la direction, et communiquée à l’ensemble des parties prenantes.

# 5. Gouvernance de la sécurité du SI

La gestion des risques constitue l’un des fondements de la politique de sécurité du CHU de La Timone. Elle vise à identifier, évaluer, hiérarchiser et maîtriser les menaces susceptibles d’affecter la confidentialité, l’intégrité, la disponibilité et la traçabilité des données, ainsi que la résilience des systèmes critiques, en cohérence avec la mission de soins et de service public hospitalier.

## 5.1. Principes directeurs

L’analyse des risques s’appuie sur les principes suivants :

* Approche globale et itérative : la gestion des risques s’applique à l’ensemble du périmètre du SI (infrastructures, logiciels, données, utilisateurs) et se renouvelle périodiquement ou en cas de changement majeur.
* Hiérarchisation des actifs critiques : classification des actifs selon leur sensibilité (ex : données de santé, SI de soins, infrastructures d’urgence) et niveau d’impact potentiel en cas de compromission.
* Proportionnalité des mesures : les dispositifs de protection sont ajustés en fonction du niveau de risque estimé, dans une logique de juste équilibre entre sécurité, coût et continuité d'activité.

## 5.2. Méthodologie d’analyse des risques

Le CHU s’appuie sur une méthodologie formelle d’analyse de risques, alignée avec les bonnes pratiques nationales (EBIOS Risk Manager, méthode ANSSI, ISO 27005). Cette méthodologie est structurée en plusieurs phases :

a) Recensement des actifs

Systèmes, applications métiers, dispositifs médicaux connectés, bases de données, réseaux, utilisateurs, processus métiers.

Identification des interconnexions (internes et externes), dépendances techniques et logiques.

b) Identification des menaces

Menaces internes : erreur humaine, négligence, malveillance interne.

Menaces externes : cyberattaques ciblées (ransomware, APT, phishing), compromission via tiers, pannes techniques, catastrophes naturelles.

Spécificité du secteur santé : menace sur les SI de soins, équipements médicaux connectés (DMNI), et chaînes logistiques critiques.

c) Évaluation des impacts

Sur les patients : interruption de soins, erreur médicale, divulgation de données personnelles sensibles.

Sur l’établissement : arrêt de l’activité, réputation, responsabilité juridique, perte financière, sanctions réglementaires.

d) Estimation de la vraisemblance

Fréquence connue d’occurrence (veille CERT Santé, retours d’incidents internes, statistiques sectorielles).

Niveau de protection existant.

e) Cartographie des risques

Élaboration de matrices de risques (gravité x probabilité).

Identification des risques majeurs (risques inacceptables nécessitant traitement immédiat).

f) Traitement des risques

Acceptation : si le risque est jugé résiduel ou tolérable.

Réduction : mise en œuvre de mesures techniques ou organisationnelles.

Transfert : par contractualisation (ex : clauses SSI dans les marchés) ou assurance.

Évitement : abandon ou refonte du processus à risque.

## 5.3. Cycles d’analyse périodique

Analyse initiale : réalisée à l’échelle globale du SI, dans le cadre du schéma directeur SSI.

Analyses projet : systématiques pour tout nouveau projet numérique (déploiement applicatif, extension d’infrastructure, interconnexion avec un prestataire externe…).

Revue annuelle : actualisation des risques identifiés, intégration de nouvelles menaces (intelligence artificielle, attaques sur les chaînes d’approvisionnement, deepfakes).

Analyse post-incident : conduite systématique après tout incident significatif pour évaluer les failles exploitées et corriger les insuffisances.

## 5.4. Responsabilités dans la gestion des risques

RSSI : responsable du pilotage global du processus, de l’animation des ateliers d’analyse, de la validation des livrables (cartographies, fiches de traitement, tableaux de bord).

Direction Générale : validation des décisions stratégiques, arbitrages budgétaires, gestion de la résilience institutionnelle.

DSI : implémentation des mesures correctives, supervision technique des contrôles.

Métiers / utilisateurs : évaluation de l’impact métier, implication dans les ateliers de cotation, appropriation des mesures de traitement.

DPO : participation dans les AIPD (analyses d’impact sur la vie privée) en cas de traitement de données personnelles.

## 5.5. Intégration dans la démarche globale de sécurité

La gestion des risques n’est pas une activité isolée, mais constitue un socle pour l’ensemble des processus SSI :

Définition des politiques : priorisation des mesures de sécurité à mettre en œuvre.

Choix des outils techniques : détection, protection, sauvegarde, cloisonnement.

Sensibilisation : ciblage des messages en fonction des risques spécifiques aux métiers (ex : risque d'hameçonnage en unité de soins).

PCA/PRA : élaboration des scénarios de crise à partir des risques les plus critiques.

# 6. Classification et gestion des actifs

La protection du système d'information repose sur un socle cohérent et complémentaire de mesures organisationnelles, techniques et physiques visant à réduire les risques identifiés. Ces mesures doivent être adaptées au contexte hospitalier du CHU de La Timone, en tenant compte des spécificités métiers, des contraintes réglementaires et des menaces cyber actuelles.

## 6.1. Mesures organisationnelles

a. Charte informatique et engagements individuels

Élaboration d’une charte informatique claire, opposable, intégrée au règlement intérieur.

Signature obligatoire pour tout utilisateur (agents, stagiaires, prestataires, partenaires).

Mise à disposition numérique et accessibilité permanente.

Sessions de rappel lors des audits, bilans de sécurité ou comités d’évaluation.

b. Gestion des habilitations et contrôle des accès

Définition précise des rôles et responsabilités dans le modèle RBAC (Role-Based Access Control).

Utilisation d’une solution de gestion des identités (IAM) avec workflow d’approbation.

Suivi automatisé du cycle de vie des comptes (création, modification, révocation).

Mécanismes de double validation pour les droits critiques (accès administrateur, données médicales).

Contrôle croisé entre les directions métier, RH et DSI.

c. Procédures de sécurité formalisées

Documentation exhaustive des procédures de gestion des incidents, changements, configurations.

Application des référentiels ITIL/SecNumCloud lorsque pertinent.

Intégration des exigences SSI dans les marchés publics, appels d’offre et comités projets.

d. Politique de sous-traitance sécurisée

Évaluation de sécurité préalable à toute contractualisation (notamment hébergeurs HDS).

Suivi de la conformité des prestataires avec des audits réguliers.

Mis en place de NDA spécifiques SSI et clauses de continuité de service en cas de rupture.

Vérification de la sécurité des solutions cloud ou SaaS utilisées.

e. Sensibilisation et formation continue

Déploiement d’un plan pluriannuel de sensibilisation adapté aux profils (technique, administratif, clinique).

Utilisation de simulateurs d’attaques de phishing et de scénarios gamifiés.

Formation obligatoire pour les référents SSI, chefs de service, chefs de projets numériques.

Évaluation continue de la maturité SSI individuelle à travers des questionnaires et audits comportementaux.

## 6.2. Mesures techniques

a. Authentification et contrôle d’accès

Mise en place d’une authentification multifacteur (MFA) pour les utilisateurs à privilèges et les accès distants.

Gestion des comptes dormants (désactivation automatique au-delà de 30 jours d’inactivité).

Surveillance des tentatives de connexions anormales via corrélation SIEM.

b. Sécurisation des postes de travail et serveurs

Déploiement d’une politique de durcissement des OS (CIS Benchmarks, ANSSI).

Blocage des périphériques non autorisés (USBGuard, politiques GPO).

Supervision continue via des agents EDR et outils de Threat Hunting.

Journalisation locale et centralisée des actions administratives.

c. Sécurité réseau

Architecture réseau cloisonnée avec DMZ, VLAN métiers, et bastions pour administration.

Supervision via des sondes de détection (IDS/IPS, honeypots).

Accès VPN avec contrôle contextuel (heure, lieu, comportement habituel).

d. Protection des applications et bases de données

Intégration du DevSecOps dans les projets applicatifs internes (CI/CD avec analyse statique et dynamique).

Mécanismes de prévention contre les injections, attaques XSS, CSRF via WAF et durcissement applicatif.

Mises à jour logicielles automatisées et validation en préproduction.

e. Sauvegarde et reprise d’activité

Déploiement d’une infrastructure de sauvegarde isolée (« air gapped » ou immutable backup).

Revue périodique de la criticité des données sauvegardées.

Inclusion de scénarios cyber (ransomware, effacement) dans les tests de PRA.

f. Surveillance et réponse aux incidents

Mise en œuvre d’un SOC interne ou mutualisé avec des alertes contextualisées.

Définition claire des SLA de traitement selon la criticité des incidents.

Tableau de bord décisionnel à destination de la direction.

Simulation d’incidents régulière (« Red Team », « Purple Team », crise cyber simulée).

## 6.3. Mesures physiques

a. Contrôle d’accès physique

Badge nominatif avec photo, code couleur selon les profils (soins, IT, prestataires).

Alarmes et contrôles renforcés pour les zones sensibles (centre de données, archives).

Revue des habilitations physiques synchronisée avec la gestion des identités numériques.

b. Sécurisation des locaux techniques

Redondance des équipements critiques (climatisation, électricité).

Surveillance environnementale temps réel (capteurs de température, humidité, détection de fuite).

Journaux de maintenance et d’accès archivés pour vérification SSI.

c. Gestion des supports et déchets

Suivi RFID ou équivalent pour les supports amovibles contenant des données de santé.

Déchiquetage ou destruction thermique certifiée des supports papier ou numériques obsolètes.

Traçabilité complète des opérations de destruction externalisées (bordereaux, audits).

# 7. Contrôle des accès et authentification

La gestion des incidents de sécurité est une composante centrale de la PSSI du CHU Ynov.

Elle vise à garantir une réponse rapide, structurée et efficace à tout événement susceptible de compromettre la confidentialité, l’intégrité, la disponibilité ou la traçabilité des systèmes d’information. Elle s'inscrit dans une logique de résilience organisationnelle et de conformité réglementaire (RGPD, PGSSI-S, RGS, etc.).

## 7.1. Définition d’un incident de sécurité

Un incident de sécurité informatique est défini comme tout événement ou série d'événements non désirés ou inattendus liés à la sécurité du système d'information, ayant un impact négatif réel ou potentiel sur celui-ci. Cela inclut notamment :

* Les attaques logicielles (malwares, ransomwares, virus, vers, chevaux de Troie).
* L’ingénierie sociale (hameçonnage/phishing, spear phishing, usurpation d’identité).
* L’accès physique non autorisé à des salles serveurs ou postes sensibles.
* Les erreurs humaines ou défaillances internes entraînant une exposition de données.
* La défaillance de dispositifs de sécurité périmétrique ou interne (firewall, antivirus, DLP, etc.).

## 7.2. Processus de gestion des incidents

Le processus de gestion suit un cycle de vie structuré selon les normes ISO/IEC 27035-1 et 27035-2, composé de plusieurs phases distinctes :

Détection et identification :

* Supervision en continu des journaux systèmes, alertes de sécurité, trafic réseau.
* Utilisation de solutions de threat intelligence pour identifier des IOC (Indicateurs de Compromission).
* Collaboration avec les CERT (Computer Emergency Response Team) nationaux et partenaires sectoriels (CERT Santé, ANSSI).

Notification et escalade :

* Communication immédiate à la cellule de veille SSI.
* Notification automatisée via outils SIEM/EDR en cas de seuil critique.
* Escalade hiérarchique en fonction du type et du périmètre de l’incident (technique, réglementaire, communicationnelle).

Analyse et investigation :

* Analyse forensique des systèmes compromis (images disque, logs, mémoire volatile).
* Évaluation des vulnérabilités exploitées et typologie des vecteurs d’attaque.
* Recherche de latéralisation sur le réseau et de persistance via TTPs adverses.

Réponse immédiate :

* Mise en œuvre de mesures correctrices temporaires (containment), incluant blocage IP, désactivation de comptes, coupure de segments réseau.
* Mise à jour ou désactivation temporaire de services à risque (VPN, FTP, accès externes).

Rétablissement :

* Nettoyage des systèmes affectés, restauration depuis des sauvegardes saines, vérification d’intégrité post-restauration.
* Renforcement temporaire ou permanent des contrôles d’accès.
* Redémarrage progressif selon la criticité des services hospitaliers associés.

Retour d’expérience (REX) et mise à jour du dispositif :

* Organisation de réunions post-mortem (Post-Incident Review) avec tous les acteurs impliqués.
* Identification de failles de détection, communication ou processus.
* Intégration des enseignements dans les plans de réponse à incident, documentation, et sensibilisation.

## 7.3. Responsabilités et coordination

RSSI : autorité opérationnelle sur la gestion des incidents, responsable de la coordination transversale.

Cellule de crise SSI : activation en cas d'incident critique, avec représentants de la DSI, direction médicale, qualité, juridique et communication.

Équipes techniques : exécutent les opérations de contournement, remédiation et restauration.

Métiers : assurent la continuité des soins et relaient les informations auprès des utilisateurs finaux.

## 7.4. Moyens techniques et logistiques

Plateforme SOC interne ou mutualisée.

Intégration du CMDB (Configuration Management Database) pour faciliter la traçabilité des actifs.

Sondes NDR (Network Detection & Response) pour l’inspection réseau temps réel.

Bases IOC régulièrement mises à jour à partir de sources OSINT et Threat Intel privées.

## 7.5. Communication en situation de crise

Plan de communication interne et externe prévu dans le PCA (Plan de Continuité d’Activité).

Diffusion rapide d’alertes SSI aux utilisateurs (affiches, mail, messagerie instantanée).

Formation des porte-paroles pour échanges avec les médias, les autorités et les usagers.

## 7.6. Suivi des incidents et indicateurs de performance

Enregistrement systématique dans un registre des incidents.

Production mensuelle de tableaux de bord SSI (nombre d’incidents, MTTR, incidents bloqués en amont, etc.).

Audit interne régulier de la conformité du processus de réponse aux incidents.

# 8. Sécurité physique et environnementale

La gestion des accès et des identités (Identity and Access Management – IAM) est un pilier fondamental de la sécurité des systèmes d’information du CHU Ynov.

Elle vise à garantir que chaque utilisateur, humain ou machine, dispose du niveau minimal de privilèges nécessaire à l’exécution de ses fonctions, dans le respect du principe du moindre privilège et de la séparation des tâches.

## 8.1. Objectifs de la politique IAM

Garantir l’authentification fiable des utilisateurs.

Assurer une gestion centralisée, cohérente et traçable des identités et des habilitations.

Prévenir l’accès non autorisé aux ressources sensibles.

Réduire les risques liés à l’accumulation de privilèges excessifs.

Répondre aux exigences réglementaires et normatives (RGPD, PGSSI-S, ISO/IEC 27001 et 27002).

## 8.2. Cycle de vie des identités

Le CHU de La Timone met en œuvre un cycle de gestion complet de l’identité numérique pour chaque acteur :

Création de l’identité :

Basée sur une source de vérité RH (annuaire LDAP, logiciel RH ou scolarité pour les internes).

Attributs obligatoires : identifiant unique, prénom/nom, entité d’appartenance, rôle, date de début/fin de contrat.

Attribution des droits :

Habilitations basées sur des rôles prédéfinis (RBAC – Role Based Access Control).

Intégration dans des groupes logiques correspondant aux métiers, unités, services ou projets.

Modification/évolution :

Les changements de poste ou de missions entraînent une réévaluation automatique ou manuelle des droits.

Le SI doit être capable d’automatiser les ajustements via un moteur de règles IAM.

Désactivation / suppression :

À l’issue d’un contrat, d’un stage ou d’un départ anticipé, les accès sont immédiatement désactivés.

Des audits automatisés vérifient l’absence d’accès actifs pour les comptes dormants.

## 8.3. Authentification et contrôles d’accès

Authentification forte :

MFA (authentification multi-facteurs) obligatoire pour les accès à distance, aux outils critiques ou aux données de santé.

Cartes CPS (Carte de Professionnel de Santé) pour l’authentification nominative des personnels médicaux.

Systèmes d’authentification centralisée :

SSO (Single Sign-On) et fédération d’identité pour simplifier les accès tout en garantissant leur sécurité.

Utilisation d’annuaires LDAP/Active Directory avec réplication sécurisée.

Contrôle d’accès logique :

ACLs (Access Control Lists) dynamiques, intégrées au SI métier et systèmes partagés (dossiers patients, messagerie, GED, etc.).

Journaux d’accès horodatés et centralisés pour analyse et vérification post-incident.

## 8.4. Revue et audit des habilitations

Revue régulière (au moins semestrielle) des droits d’accès par les managers et la DSI.

Mise en œuvre de campagnes de recertification automatisées (recertification des comptes et des privilèges).

Identification et traitement des comptes orphelins, dormants, à privilèges étendus ou anormaux.

Conservation des journaux d’audit conformément à la politique de journalisation (section 11).

## 8.5. Gestion des accès privilégiés (PAM – Privileged Access Management)

Comptes à privilèges fortement contrôlés, tracés et cloisonnés (administrateurs, comptes techniques, services critiques).

Bastion d’administration (jump server) avec enregistrement des sessions et délégation granulaire.

Rotation régulière des mots de passe, génération automatique et stockage dans un coffre-fort numérique (vault).

Interdiction de l’utilisation de comptes partagés sans mécanisme de traçabilité nominative.

## 8.6. Accès des prestataires et tiers

Mise en œuvre de contrats définissant les périmètres, durées, obligations et responsabilités d’accès aux SI.

Accès via VPN avec authentification forte, filtrage IP et horodatage des connexions.

Supervision accrue des accès tiers avec alertes en cas de comportements suspects.

## 8.7. Sensibilisation et formation

Formation obligatoire à la politique de gestion des accès pour tout nouvel agent ou utilisateur externe.

Rappels réguliers sur les bonnes pratiques d’authentification (choix de mots de passe, MFA, verrouillage de session).

Affichages explicatifs dans les locaux et plateformes e-learning mises à disposition.

## 8.8. Outils de support IAM

Outils de provisioning/déprovisionnement automatisés.

Solution IAM centralisée intégrée à l’annuaire d’entreprise et aux outils métiers.

Interfaces de délégation sécurisée pour les responsables d’équipe (demande et validation d’habilitations).

# 9. Sécurité des communications et réseaux

La politique de sauvegarde, de continuité et de reprise d’activité (PCRA) vise à garantir la résilience du système d'information du CHU Ynov face aux incidents majeurs, sinistres ou cyberattaques susceptibles d'interrompre ou d'altérer les services critiques de soins, d'administration, de recherche et de pilotage.

Cette politique s’inscrit dans une démarche globale de gestion de la continuité d’activité (GCA) selon les normes ISO 22301, ISO/IEC 27031 et les recommandations de la PGSSI-S.

## 9.1. Objectifs stratégiques

Assurer l’intégrité, la disponibilité et la confidentialité des données sauvegardées.

Garantir la continuité des services critiques hospitaliers en cas d’incident majeur.

Réduire au minimum le temps d’interruption (RTO) et la perte de données admissible (RPO).

Permettre une reprise rapide, structurée et sécurisée du SI après sinistre.

Répondre aux obligations réglementaires (PGSSI-S, CNIL, code de la santé publique, etc.) en matière de sauvegarde des données de santé.

## 9.2. Politique de sauvegarde

### 9.2.1. Typologie des données sauvegardées

Données de santé à caractère personnel (dossiers patients, imagerie, biologie, etc.).

Données de gestion hospitalière (GHT, comptabilité, RH, SI achat, etc.).

Données administratives, logs, configurations critiques et VM.

Données issues de dispositifs médicaux connectés.

### 9.2.2. Principes de sauvegarde

Sauvegardes régulières, automatisées et vérifiées (quotidiennes, hebdomadaires, mensuelles).

Stratégie 3-2-1 : 3 copies de chaque donnée, sur 2 supports différents, dont 1 hors site.

Sauvegardes cryptées au repos et en transit.

Conservation sur infrastructure dédiée isolée du réseau de production (air gap ou immutable backup).

Tests de restauration périodiques pour valider l’efficacité des sauvegardes (au moins trimestriels).

Conservation des journaux de sauvegarde (horodatage, intégrité, succès/échecs).

### 9.2.3. Outils et technologies

Solutions de sauvegarde centralisées avec orchestration multi-site.

Intégration avec les hyperviseurs, bases de données, messageries et systèmes métiers.

Support des snapshots, réplications, et déduplication pour réduire les volumes.

## 9.3. Politique de continuité d’activité (PCA)

### 9.3.1. Identification des processus critiques

Cartographie des processus hospitaliers (soins, urgences, bloc, SI patients, etc.).

Définition du niveau de criticité (vital, majeur, support).

Rédaction de Plans de Continuité d’Activité spécifiques par direction ou service.

### 9.3.2. Mesures de continuité

Redondance matérielle (clusters, data centers, onduleurs, etc.).

Réplication synchrone/asynchrone entre sites (SIH, dossiers médicaux, services critiques).

Environnements de secours (shadow IT, serveurs miroir, VDI, etc.).

Procédures papiers et formulaires de secours pour les soins en cas de perte d’accès au SI.

Fourniture de réseaux de secours (4G/5G, accès WAN redondés).

### 9.3.3. Maintenance du PCA

Mise à jour annuelle du PCA.

Exercices réguliers (tests de bascule, simulations de panne, crash tests).

Revue avec la cellule de gestion de crise hospitalière.

## 9.4. Politique de reprise d’activité (PRA)

### 9.4.1. Objectifs du PRA

Rétablir un état opérationnel minimal des services numériques critiques.

Assurer une relance progressive et contrôlée des systèmes après incident.

### 9.4.2. Plan de Reprise Informatique (PRI)

Rédaction de scénarios de reprise par type d’incident (cyberattaque, incendie, panne électrique, etc.).

Priorisation des systèmes à restaurer selon un classement par criticité (SIH, PACS, LIMS, etc.).

Disponibilité de documentation technique et procédures de restauration pour chaque système.

Automatisation des séquences de redémarrage lorsque possible.

### 9.4.3. Environnements de secours

Data center secondaire avec infrastructures prêtes à accueillir les restaurations.

Réseau et sécurité reconfigurables (firewall, VPN, DNS) en PRA.

### 9.4.4. Reprise après cyberattaque

Procédure de "clean build" (reconstruction à partir d’images saines et contrôlées).

Validation de l’intégrité avant réintégration sur le réseau.

Coordination avec l’ANSSI, la cellule de crise cyber et la DPO.

## 9.5. Organisation et responsabilités

RSSI : pilote les PCA/PRA, définit les exigences de sauvegarde.

DSI : met en œuvre les outils techniques, supervise les opérations et tests.

Métiers / directions : participent à la cartographie des processus critiques.

Direction générale : valide les plans, alloue les budgets, déclenche les crises.

Équipe de gestion de crise : coordination transversale en cas d’incident majeur.

## 9.6. Tests, audits et amélioration continue

Tests annuels du PRA (technique) et exercices de simulation du PCA (organisationnels).

Audits internes réguliers sur la qualité, fréquence et efficacité des sauvegardes/restaurations.

Suivi des indicateurs RTO, RPO, disponibilité des données, erreurs de sauvegarde.

Mise à jour continue des procédures après chaque incident ou exercice.

# 10. Sécurité des systèmes et applications

## 10.1. Objectifs généraux

Garantir la sécurité des équipements informatiques, biomédicaux et dispositifs médicaux connectés (DMC) constitue une priorité stratégique pour assurer la qualité et la sécurité des soins, la confidentialité des données de santé, et la continuité des activités cliniques au CHU Ynov. Cette politique vise à :

* Prévenir les risques de compromission (intrusion, altération, dysfonctionnement) des dispositifs connectés.
* Assurer une gestion rigoureuse de leur cycle de vie (acquisition, déploiement, maintenance, mise hors service).
* Intégrer les DMC dans la stratégie globale de cybersécurité et dans le système d’information hospitalier (SIH).

## 10.2. Inventaire et classification

Tous les dispositifs médicaux connectés doivent être référencés dans un inventaire centralisé (CMDB).

Chaque DMC est classifié selon son niveau de criticité (impact patient, accès au réseau, sensibilité des données traitées).

Une évaluation de la surface d’attaque est conduite à l’entrée dans le parc (audit de sécurité, analyse de conformité).

## 10.3. Sécurisation à l’acquisition

Les critères de cybersécurité sont intégrés aux cahiers des charges d’achat (ISO 81001, clause cybersécurité).

Validation par la DSI/RSSI avant tout achat ou déploiement.

Exigence de certifications ou labels (ex : CE, FDA avec exigences de sécurité intégrées).

## 10.4. Intégration au réseau hospitalier

Les DMC sont intégrés dans des VLAN dédiés, segmentés selon les familles de dispositifs (imagerie, monitoring, blocs, etc.).

Accès au SI limité par des ACL spécifiques (pas d’accès direct aux données sensibles sans proxy ou passerelle sécurisée).

Surveillance des flux réseau par IDS/IPS spécifiques (détection comportementale).

## 10.5. Gestion des mises à jour et correctifs

Politique de patch management adaptée aux DMC en concertation avec les fournisseurs.

Les mises à jour sont testées et planifiées avec les unités cliniques pour éviter les interruptions de soins.

Contrat de maintenance intégrant les délais de correction des vulnérabilités critiques.

## 10.6. Authentification et accès

Mise en œuvre d’un contrôle d’accès logique pour les interfaces d’administration (login nominatif, MFA si possible).

Journalisation de toutes les actions effectuées sur les dispositifs (connexion, configuration, logs cliniques).

Interdiction de comptes partagés ou par défaut (obligation de reconfiguration initiale).

## 10.7. Surveillance et supervision

Intégration des DMC aux outils de supervision de l’infrastructure (métrologie, alertes, comportements anormaux).

Surveillance de l’usage avec alertes en cas de comportement déviant (arrêt inopiné, pics d’activité).

Audit de configuration et revue de conformité régulière.

## 10.8. Fin de vie et décommissionnement

Procédure de retrait sécurisée (effacement des données, désactivation réseau, retrait de l’inventaire).

Décontamination logicielle et matérielle conformément aux exigences du RGPD et des procédures hospitalières.

Destruction ou recyclage selon des procédures certifiées (traçabilité complète).

## 10.9. Sensibilisation et collaboration

Collaboration étroite entre la direction biomédicale, la DSI, la cellule SSI et les unités cliniques.

Sensibilisation des utilisateurs à l’usage sécurisé des DMC.

Veille technologique et réglementaire sur les nouvelles menaces affectant les dispositifs médicaux connectés.

# 11. Protection contre les logiciels malveillants

## 11.1. Objectifs

La politique de journalisation et de traçabilité vise à assurer la transparence, la responsabilisation et la détection proactive des événements anormaux ou malveillants au sein du SIH. Elle constitue un levier essentiel pour :

Assurer la conformité aux exigences réglementaires (notamment le RGPD, l'instruction MSSSI, les référentiels de l'ANSSI et de la CNIL).

Permettre la détection rapide d'incidents ou de comportements suspects.

Faciliter l'investigation en cas d'incident de sécurité ou de dysfonctionnement.

Garantir la non-répudiation des actions critiques sur le SI.

## 11.2. Périmètre de la journalisation

Tous les systèmes et équipements participant au traitement des données du SIH doivent disposer de capacités de journalisation, notamment :

Les serveurs (systèmes d’exploitation, bases de données, applications critiques).

Les postes de travail et terminaux mobiles accédant à des ressources sensibles.

Les dispositifs réseau (pare-feux, routeurs, commutateurs, équipements Wi-Fi, VPN).

Les dispositifs biomédicaux connectés.

Les services Cloud et systèmes externalisés.

## 11.3. Événements à journaliser

Les journaux doivent permettre de tracer notamment :

Les tentatives d’authentification (réussies ou échouées).

Les accès aux données de santé ou systèmes critiques.

Les modifications de droits, de configurations ou d’infrastructures.

Les opérations administratives sensibles (redémarrages, patchs, suppressions, exports de données).

Les transferts de données internes ou externes.

Les connexions VPN, rebonds, sessions distantes (RDP, SSH, etc.).

## 11.4. Conditions de journalisation

Les horodatages doivent être synchronisés via un serveur NTP centralisé (traçabilité temporelle uniforme).

Les logs doivent être horodatés avec précision, signés numériquement si besoin.

Les journaux doivent être horodatés en UTC+1/+2 avec détection de falsification.

## 11.5. Centralisation et conservation

Les journaux critiques doivent être centralisés dans un système SIEM (Security Information and Event Management).

La conservation minimale est de 12 mois pour tous les journaux critiques, et jusqu’à 36 mois pour certaines opérations sensibles ou réglementées.

Les journaux doivent être protégés contre la suppression, la modification non autorisée ou l’effacement accidentel.

## 11.6. Accès aux journaux

L’accès aux journaux est strictement réservé au personnel autorisé (RSSI, administrateurs sécurité, auditeurs habilités).

Toute consultation doit être tracée, avec journalisation secondaire des requêtes et accès.

Des audits périodiques sont réalisés pour s'assurer du respect des conditions d’accès et d’exploitation des logs.

## 11.7. Analyse et exploitation

Des tableaux de bord de sécurité sont générés automatiquement à partir des journaux.

Les corrélations d’événements sont configurées dans le SIEM pour détecter :

Des élévations de privilèges suspectes.

Des comportements anormaux (horaires atypiques, exfiltration de données, etc.).

Des attaques connues (pattern de ransomware, scans réseau, etc.).

En cas d’incident, une copie des logs est gelée, analysée et horodatée pour intégration dans un dossier d’investigation.

## 11.8. Formation et sensibilisation

Les administrateurs, développeurs et référents métiers sont formés aux obligations de traçabilité.

Des sessions de sensibilisation internes sont régulièrement organisées pour rappeler les enjeux de la journalisation.

## 11.9. Évolutivité et conformité continue

La politique de journalisation est revue annuellement, intégrant les évolutions réglementaires, technologiques et les retours d’expérience.

Un plan d’amélioration continue de la traçabilité est piloté par la cellule SSI.

# 12. Gestion des incidents de sécurité

## 12.1. Objectifs

La sécurité des projets informatiques et applicatifs vise à garantir que toute évolution ou mise en place de solutions informatiques respecte les exigences de sécurité du CHU Ynov dès les phases amont de conception, en intégrant les principes de « Security by Design » et « Privacy by Design ».

## 12.2. Intégration de la sécurité dans le cycle de vie des projets (SDLC)

Phase de cadrage : chaque projet est soumis à une analyse de risque SSI et à une étude d’impact sur la vie privée (EIVP) si des données à caractère personnel sont traitées.

Phase de conception : des exigences de sécurité (chiffrement, authentification forte, segmentation, etc.) sont formalisées dans les cahiers des charges.

Phase de développement : les bonnes pratiques de développement sécurisé sont appliquées (OWASP Top 10, durcissement des bibliothèques, etc.). Des revues de code et tests de sécurité sont planifiés.

Phase de recette : des tests d’intrusion, scans de vulnérabilités, tests d’acceptation de sécurité (SAT) sont menés avec le concours de la cellule SSI.

Phase de mise en production : les livrables doivent être accompagnés de leur documentation de sécurité, journalisation active, supervision intégrée, et plan de continuité.

Phase de maintenance : les correctifs de sécurité doivent être intégrés dans le cycle de MCO (maintien en condition opérationnelle) avec une gestion proactive des vulnérabilités.

## 12.3. Gouvernance des projets SSI

Tous les projets IT doivent être référencés auprès de la DSI et du RSSI.

Un référent SSI est désigné pour chaque projet critique afin de garantir le respect des exigences SSI.

Le comité de pilotage SSI peut suspendre un projet ne répondant pas aux exigences minimales de sécurité.

## 12.4. Documentation et traçabilité

Un dossier de sécurité de projet est établi, comportant :

L’analyse de risques SSI

Le plan de traitement des risques

Les tests de sécurité réalisés

Les plans de secours et de reprise associés

Les engagements des prestataires en matière de sécurité

Ce dossier est conservé et mis à jour durant tout le cycle de vie du projet.

## 12.5. Projets externalisés ou SaaS

Tout projet reposant sur des solutions cloud, hébergements externes ou prestataires doit :

Respecter les règles de souveraineté, de localisation des données et d’hébergement certifié HDS.

Inclure dans les contrats des clauses spécifiques SSI (exigences de conformité, réversibilité, auditabilité, etc.).

Être audité avant intégration au SIH et validé par le RSSI.

## 12.6. Évaluation continue

Des audits annuels des projets actifs sont réalisés pour détecter les écarts de sécurité.

Des retours d’expérience (REX) sont collectés en fin de projet pour améliorer les pratiques SSI.

# 13. Continuité d’activité et reprise après sinistre

## 13.1. Objectifs

Le développement d’une culture de cybersécurité constitue un pilier fondamental de la PSSI. L’objectif est de faire de chaque collaborateur un maillon actif de la protection du système d’information, en inculquant une compréhension claire des enjeux, des comportements à adopter, et des menaces à éviter.

Cette démarche vise :

À réduire les comportements à risque en sensibilisant les utilisateurs aux bonnes pratiques.

À renforcer la capacité de détection précoce des incidents.

À accroître l’adhésion des équipes aux règles de sécurité.

À garantir la conformité aux obligations réglementaires en matière de formation et de sensibilisation.

## 13.2. Publics cibles

Tous les utilisateurs du SIH sont concernés, avec des modules adaptés aux profils suivants :

Personnel médical et paramédical

Agents administratifs

Techniciens et ingénieurs informatiques

Direction générale et responsables métiers

Prestataires, sous-traitants et partenaires externes

## 13.3. Contenus pédagogiques et thématiques abordées

Les actions de sensibilisation couvriront les domaines suivants :

Règles fondamentales de cybersécurité (mots de passe, verrouillage de poste, etc.)

Phishing et ingénierie sociale

Gestion des supports amovibles

Utilisation sécurisée de la messagerie professionnelle

Accès distants et télétravail sécurisé

Confidentialité des données de santé

Procédures en cas de suspicion d’incident ou de fuite

Responsabilités juridiques et réglementaires

Des modules spécifiques seront également développés pour les fonctions sensibles (ex. administrateurs systèmes, développeurs, chercheurs manipulant des données sensibles, etc.).

## 13.4. Moyens pédagogiques

Plateforme e-learning accessible en ligne

Ateliers en présentiel animés par la cellule SSI

Sessions de simulation de phishing

Affichages et supports de communication interne (affiches, guides, bulletins de sensibilisation)

Intégration dans les parcours d’intégration des nouveaux arrivants

Journées dédiées à la cybersécurité (CyberDays)

## 13.5. Suivi, évaluation et amélioration

Un plan annuel de formation SSI est établi et suivi par la DSI et le RSSI

Des indicateurs de suivi (taux de complétion, résultats aux quiz, feedback utilisateurs) sont collectés

Des bilans annuels sont présentés au Comité de pilotage SSI

Les supports sont mis à jour annuellement en fonction de l’évolution des menaces et des retours d’expérience

## 13.6. Responsabilités

Le RSSI coordonne les campagnes de sensibilisation et valide les contenus.

La DRH intègre la formation SSI dans les plans de formation institutionnels.

La DSI et les chefs de service relaient les campagnes et veillent à la participation effective de leurs équipes.

# 14. Sensibilisation et formation des utilisateurs

## 14.1. Objectifs

Le CHU Ynov collabore avec de nombreux tiers, notamment des prestataires, fournisseurs, partenaires institutionnels, établissements de santé, organismes de recherche et éditeurs de logiciels. Cette diversité d'interactions crée un périmètre élargi de risques qu'il est nécessaire de maîtriser à travers une gestion rigoureuse des relations contractuelles, techniques et organisationnelles.

Les objectifs de cette politique sont les suivants :

Encadrer les relations avec les tiers pour assurer la confidentialité, l'intégrité et la disponibilité du SI.

Garantir que les exigences de sécurité soient systématiquement intégrées dans les contrats et conventions.

Contrôler les accès et les activités des tiers au sein du SI du CHU.

Limiter les risques de compromission, de perte ou de fuite d’informations liées aux interventions externes.

## 14.2. Typologie des tiers concernés

Prestataires techniques (infogérance, maintenance, support applicatif)

Fournisseurs de services cloud (IaaS, SaaS, PaaS)

Partenaires scientifiques et académiques (recherche biomédicale, collaboration inter-hospitalière)

Organismes publics (ARS, CNAM, ANS, etc.)

Sociétés de conseil et d’expertise

Sous-traitants manipulant des données de santé ou accédant aux SIH

## 14.3. Exigences contractuelles de sécurité

Tout contrat ou convention doit inclure un volet sécurité contenant au minimum :

Des clauses de confidentialité spécifiques aux données de santé et informations sensibles.

Des engagements relatifs à la conformité RGPD et au respect des référentiels de sécurité (PGSSI-S, ISO 27001).

La définition des niveaux d’habilitation, périmètre d’accès, durée et traçabilité.

Une clause de notification obligatoire en cas d’incident ou de faille de sécurité.

Des droits de contrôle, d’audit ou d’inspection à la charge du CHU.

## 14.4. Processus d’intégration et de suivi des tiers

Validation des contrats par la direction juridique et le RSSI.

Enregistrement des tiers dans un référentiel de partenaires avec un identifiant unique.

Réalisation d’une analyse de risques avant toute connexion au SI.

Mise en place de procédures de contrôle d’accès spécifiques pour les comptes tiers (comptes nominatifs, temporaires, restreints).

Désactivation ou suppression des accès à la fin de la mission ou du contrat.

Audits de conformité périodiques des prestations sensibles.

## 14.5. Responsabilités

Le RSSI assure le contrôle des exigences SSI dans les relations avec les tiers.

Le Département des Achats veille à la bonne intégration des clauses SSI dans les contrats.

Les chefs de projet ou responsables métiers assurent la coordination opérationnelle et le suivi des interventions des tiers.

Le service juridique valide les engagements contractuels liés à la sécurité.

## 14.6. Mesures spécifiques en cas de sous-traitance

Lorsqu’un tiers fait appel à un sous-traitant, le CHU exige que les obligations de sécurité soient portées par effet miroir. Toute chaîne de sous-traitance doit être :

Connue et documentée.

Approuvée par le CHU.

Suivie dans le cadre d’un contrôle renforcé.

Le non-respect de ces exigences pourra conduire à une suspension ou à une rupture contractuelle.

# 15. Sécurité des prestataires et des tiers

## 15.1. Objectif

Garantir la résilience, la réactivité et la continuité des activités critiques du CHU de La Timone en cas de crise affectant le système d'information, qu'elle soit d'origine interne (panne majeure, erreur humaine) ou externe (attaque cyber, catastrophe naturelle, mouvement social, etc.).

## 15.2. Définition de la situation de crise SI

Une crise SI est caractérisée par un événement ou une série d’événements qui compromet gravement la disponibilité, la confidentialité ou l'intégrité des systèmes d'information au point de perturber le fonctionnement normal des services hospitaliers, médicaux, ou administratifs.

## 15.3. Préparation et anticipation

Élaboration et maintien à jour d’un Plan de Continuité d’Activité (PCA) et d’un Plan de Reprise d’Activité Informatique (PRAI).

Cartographie des processus critiques dépendant du SI.

Définition des scénarios de crise les plus probables : ransomware, indisponibilité réseau, compromission d’un système central (DPI, laboratoire, radiologie, etc.).

Constitution d’une cellule de crise SSI composée du RSSI, DSI, représentants de la direction générale, communication et sécurité physique.

Mise en place d’exercices de simulation de crise (table-top, tests techniques, alertes réelles simulées).

## 15.4. Organisation de la gestion de crise

Déclenchement formalisé par le RSSI ou le DSI en fonction du niveau de gravité.

Activation des chaînes d’alerte internes et externes (ARS, ANS, CERT Santé).

Mise en œuvre de l’arbre décisionnel du PCA/PRAI.

Communication de crise : messages préparés, canaux alternatifs identifiés (téléphone, radio, documents papier).

Journalisation de tous les événements liés à la crise pour analyse post-incident.

## 15.5. Outils et ressources dédiés

Infrastructures de secours (site de repli, hébergement secondaire).

Réseaux segmentés et équipements de communication de secours.

Plateformes d’orchestration de crise.

Kits de reprise : documentation imprimée, systèmes manuels, liste de contacts prioritaires.

## 15.6. Reprise d’activité et retour à la normale

Phasage de la reprise en fonction des priorités cliniques et logistiques.

Validation de l’intégrité des données avant toute réactivation.

Désinfection complète des systèmes contaminés (en cas de cyberattaque).

Analyse post-mortem pour formaliser les retours d’expérience (RETEX).

Intégration des leçons apprises dans les processus de prévention, formation, PCA et PRAI.

## 15.7. Responsabilités

Le RSSI est responsable de la coordination SSI de la crise.

La DSI assure le support technique et l’application des procédures de PRAI.

Le Directeur de crise assure l’arbitrage stratégique et la communication vers les tutelles.

Les chefs de pôles métiers assurent la continuité organisationnelle au sein des services cliniques et administratifs.

## 15.8. Amélioration continue

Révision annuelle des PCA/PRAI avec prise en compte des nouvelles menaces.

Évaluation régulière de la maturité de la gestion de crise.

Capitalisation des RETEX pour faire évoluer les pratiques.

# 16. Conformité, audit et amélioration continue

## 16.1. Objectifs

L’objectif de cette section est de garantir l’efficacité, la conformité et l’amélioration continue des mesures de sécurité en place au sein du CHU Ynov à travers un dispositif structuré de surveillance, d’audit et de contrôle interne. Elle permet également d’identifier les écarts par rapport à la politique de sécurité, d’évaluer le niveau de maturité SSI, et de démontrer la conformité réglementaire et normative.

## 16.2. Dispositif de surveillance

Mise en œuvre de solutions de supervision centralisée (SIEM) pour la détection des événements anormaux.

Intégration de tableaux de bord de sécurité permettant un suivi en temps réel des indicateurs clés (indicateurs d’alerte, tentatives de compromission, taux de conformité, etc.).

Surveillance des flux réseaux, des journaux systèmes, des accès sensibles et des comportements utilisateurs.

Intégration d’outils de détection d’intrusion (IDS/IPS), antivirus, antimalware, EDR/XDR, et filtrage DNS pour couvrir l’ensemble des périmètres SI.

Surveillance spécifique des systèmes critiques (DPI, imagerie, laboratoire, dispositifs médicaux).

## 16.3. Audit de sécurité

Élaboration d’un programme pluriannuel d’audits internes SSI en cohérence avec les exigences de la HDS, de la norme ISO 27001, et des obligations du RGPD.

Réalisation d’audits techniques (tests d’intrusion, revues de code, audits de configuration, évaluation de la surface d’exposition).

Audits organisationnels (revue des procédures, plans de continuité, gestion des identités, sensibilisation).

Recours à des audits externes réguliers par des prestataires certifiés PASSI (prestataires d’audit de sécurité des SI).

Suivi de la mise en œuvre des recommandations issues des audits via un plan d’action SSI intégré au plan d’amélioration continue.

## 16.4. Contrôles internes

Déploiement de contrôles périodiques automatisés (vérifications de configuration, scans de vulnérabilités, conformité aux référentiels techniques).

Réalisation de revues de droits d’accès trimestrielles.

Vérification de l’application des politiques de gestion des mots de passe, du chiffrement, des mises à jour et des correctifs de sécurité.

Évaluation périodique des performances des dispositifs de sécurité (taux de blocage, faux positifs, détection des menaces, temps de réponse).

Intégration des résultats dans le tableau de bord SSI présenté en Comité de Pilotage SSI (Copil SSI).

## 16.5. Responsabilités

Le RSSI supervise l’ensemble des activités de surveillance et d’audit.

La DSI assure le déploiement des outils techniques et le maintien opérationnel du dispositif de contrôle.

Le service Qualité, les auditeurs internes et les prestataires externes interviennent selon une planification définie.

Les métiers sont responsables de la conformité de leurs processus et de l’application des recommandations les concernant.

## 16.6. Amélioration continue

Analyse des résultats d’audits et de contrôles pour orienter la politique SSI.

Mise à jour annuelle du plan de surveillance et d’audit en fonction de l’évolution des risques, des technologies, des incidents constatés et des évolutions réglementaires.

Communication régulière des résultats et des alertes au Comité de Direction, aux instances métiers et aux tutelles.

# 17. Annexe – Documents de référence

Cette section liste les documents de référence, normes, guides et procédures internes qui appuient, complètent ou détaillent la mise en œuvre de la présente PSSI. Ces annexes peuvent être mises à jour de manière indépendante de la PSSI, sous contrôle du RSSI.

## 17.1. Documents internes

Charte d’utilisation des systèmes d’information de l’AP-HM

Plan de continuité d’activité (PCA) et plan de reprise d’activité (PRA)

Procédures de gestion des incidents de sécurité

Procédure de gestion des droits d’accès

Politique de sauvegarde et d’archivage

Règlement intérieur de l’établissement (mentionnant les obligations SSI)

Registre des traitements RGPD

Cartographie des actifs du SI et des traitements associés

Registre des incidents de sécurité

Dossier d’architecture du SI

Politique de gestion des mots de passe

Procédure d’accueil et de départ des agents

## 17.2. Référentiels et normes externes

Règlement Général sur la Protection des Données (RGPD – UE 2016/679)

Loi Informatique et Libertés (modifiée)

Référentiel HDS (Hébergeur de Données de Santé)

Normes ISO/IEC 27001, 27002, 27005, 27799 (sécurité de l’information, gestion des risques et données de santé)

Guides de l’ANSSI (Agence nationale de la sécurité des systèmes d'information) : classification des données, bonnes pratiques de sécurité, référentiels PSSI

Bonnes pratiques de l’ENISA (Agence européenne pour la cybersécurité)

Doctrine de sécurité des systèmes d’information de santé (Ministère de la Santé – DNS)

## 17.3. Cadres contractuels

Clauses de sécurité des contrats fournisseurs (prestations de maintenance, cloud, infogérance, etc.)

Engagements de confidentialité

Contrats de sous-traitance informatique

Conventions de mise à disposition ou de transfert de données avec des tiers (partenaires, chercheurs, institutions)

## 17.4. Maintenance et diffusion des annexes

Les documents listés sont tenus à jour par le RSSI et les référents concernés (DSI, DPO, qualité, etc.).

L’ensemble des documents est disponible sur l’intranet du CHU, dans un espace sécurisé réservé aux personnels habilités.

Les mises à jour importantes sont communiquées via les canaux institutionnels (notes internes, email, réunions d’encadrement).

# 18. Entrée en vigueur

La présente politique entre en vigueur à la date de sa validation officielle. Elle est applicable à l’ensemble des acteurs mentionnés et engage leur responsabilité individuelle et collective.

Tout manquement à cette politique pourra faire l’objet de sanctions disciplinaires ou contractuelles conformément aux règles internes de l’établissement.