Projet fil rouge - Bachelor 3 : Cybersécurité

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (PSSI)

Administrateur Systèmes, Réseaux et Sécurité

Réalisé par :

Clément Garcia
Nils Jaudon
Yann Blanc

Ynov Informatique

15 avril 2025 **Version du document validé par Michel Gournier :** 1.5

Table des matières :

1. Introduction

1.1. Contexte et Objectifs

La Politique de Sécurité des Systèmes d'Information (PSSI) de l'hôpital constitue le socle fondamental de la stratégie de protection numérique de notre établissement. Elle vise à garantir :
— La protection des données de santé des patients contre tout accès non autorisé
— La continuité des soins et le fonctionnement ininterrompu des services médicaux
— La conformité avec les exigences légales et réglementaires (RGPD, HDS, normes ISO 27001)
— La préservation de la confiance des patients et partenaires

1.2. Enjeux Spécifiques au Secteur Hospitalier

Notre établissement fait face à des défis particuliers :
— La criticité des systèmes d'information dans la chaîne de soins
— La sensibilité extrême des données de santé traitées
— La nécessité d'un équilibre entre sécurité et accessibilité des informations médicales
— L'émergence de nouvelles menaces ciblant spécifiquement le secteur hospitalier
— L'intégration croissante de dispositifs médicaux connectés

1.3. Engagement de la Direction

La direction de l'hôpital s'engage formellement à :
— Soutenir pleinement la mise en œuvre de cette politique
— Allouer les ressources humaines, techniques et financières nécessaires
— Promouvoir une culture de sécurité à tous les niveaux de l'organisation
— Participer activement au suivi de l'efficacité des mesures de sécurité
— contexte

---

2. Périmètre

2.1. Systèmes et Infrastructures Concernés

Cette PSSI s'applique à l'ensemble des composantes du système d'information :

2.1.1. Données et Applications

— Dossier Patient Informatisé (DPI) et ses modules (prescriptions, résultats d'examens)
— Systèmes d'Information Radiologique (SIR) et d'archivage PACS
— Logiciels de gestion administrative et financière
— Applications mobiles professionnelles utilisées par le personnel soignant
— Messageries sécurisées de santé
— Données de recherche clinique et biobanques numériques

2.1.2. Infrastructures Techniques

— Serveurs physiques et virtuels hébergeant les applications critiques
— Infrastructure de stockage primaire et secondaire
— Réseaux filaires (LAN) et sans fil (WLAN)
— Équipements de sécurité périmétrique (pare-feu, proxys, VPN)
— Systèmes de télécommunication (téléphonie IP, visioconférence)
— Systèmes de contrôle d'accès physique liés à l'informatique

2.1.3. Équipements Médicaux

— Dispositifs médicaux connectés (pompes à perfusion, moniteurs de surveillance)
— Équipements d'imagerie médicale (IRM, scanner, échographes)
— Équipements de bloc opératoire connectés
— Robots chirurgicaux et systèmes d'assistance opératoire
— Systèmes de télémédecine et télésurveillance

2.1.4. Terminaux Utilisateurs

— Postes de travail fixes et portables
— Tablettes et smartphones professionnels
— Terminaux d'accès partagés dans les services
— Équipements des prestataires connectés temporairement au réseau

2.2. Acteurs Concernés

La PSSI s'applique à l'ensemble des personnes physiques ou morales interagissant avec le système d'information :
— Personnel médical (médecins, chirurgiens, anesthésistes)
— Personnel paramédical (infirmiers, aides-soignants, techniciens)
— Personnel administratif et technique
— Étudiants et stagiaires
— Patients accédant à leurs données via le portail patient
— Prestataires externes et sous-traitants
— Partenaires de santé (autres établissements, laboratoires)
— Organismes de recherche collaborant avec l'hôpital

2.3. Limites du Périmètre

Cette politique ne couvre pas :
— Les systèmes personnels des employés non connectés au réseau de l'hôpital
— Les applications grand public utilisées par les patients en dehors du cadre hospitalier
— Les systèmes de partenaires externes interconnectés mais non administrés par l'hôpital

---

3. Principes Généraux

3.1. Approche par les Risques

Notre politique de sécurité s'appuie sur une démarche d'analyse des risques :
— Identification systématique des actifs critiques et de leurs vulnérabilités
— Évaluation régulière des menaces potentielles et de leurs impacts
— Priorisation des mesures de sécurité selon la criticité des risques
— Documentation formelle des analyses de risques et revue annuelle

3.2. Principes Fondamentaux de Sécurité

3.2.1. Confidentialité

— Classification des données selon leur sensibilité (critique, sensible, interne, publique)
— Cloisonnement des accès selon le principe du "besoin d'en connaître"
— Chiffrement systématique des données sensibles au repos et en transit
— Procédures de vérification d'identité renforcées pour les accès distants

3.2.2. Intégrité

- Mécanismes de contrôle d'intégrité des données cliniques
- Validation des modifications par signature électronique qualifiée
- Procédures de réconciliation des données entre systèmes
- Pistes d'audit inaltérables pour toute modification de données médicales

3.2.3. Disponibilité

- Architecture hautement disponible pour les applications critiques (99,9%)
- Redondance des infrastructures réseau et énergétiques
- Procédures de sauvegarde multicouches et tests de restauration réguliers
- Plans de secours informatique formalisés et testés

3.2.4. Traçabilité

- Journalisation centralisée de toutes les actions significatives
- Conservation des logs pendant la durée légale (minimum 12 mois)
- Horodatage fiable de toutes les transactions
- Alerte automatique en cas d'accès anormaux aux données sensibles

3.3. Principes d'Architecture Sécurisée

- Défense en profondeur avec plusieurs couches de protection
- Segmentation réseau par type de services et niveau de criticité
- Principe de moindre privilège pour tous les comptes utilisateurs
- Conception sécurisée pour toute nouvelle application (Security by Design)
- Durcissement systématique des systèmes exposés

---

4. Gouvernance et Organisation de la Sécurité

4.1. Structure Organisationnelle

4.1.1. Comité de Sécurité du Système d'Information

- **Composition** : Direction Générale, DSI, RSSI, DPO, représentants des services médicaux
- **Fréquence** : Réunion trimestrielle
- **Missions** :
  - Valider la stratégie de sécurité et ses évolutions
  - Arbitrer les investissements en matière de sécurité
  - Suivre les indicateurs de performance de la sécurité
  - Examiner les incidents majeurs et valider les plans d'action

4.1.2. Équipe Opérationnelle de Sécurité

- **Composition** : RSSI, administrateurs sécurité, référents sécurité métiers
- **Fréquence** : Réunion mensuelle
- **Missions** :
  - Mettre en œuvre les mesures de sécurité techniques
  - Assurer la veille sur les vulnérabilités et menaces
  - Conduire les tests de sécurité réguliers
  - Proposer des améliorations techniques

4.2. Rôles et Responsabilités

4.2.1. Direction Générale

- Porte la responsabilité juridique finale de la sécurité des données
- Valide la PSSI et ses mises à jour majeures
- Alloue les ressources nécessaires à la mise en œuvre de la PSSI (budget annuel dédié à la sécurité $\geq 6\%$ du budget IT)
- Arbitre les situations exceptionnelles nécessitant une dérogation à la PSSI

— Préside le Comité de Sécurité du Système d'Information trimestriel
— Approuve formellement le plan de traitement des risques majeurs
— Signe les déclarations de conformité réglementaire (RGPD, HDS)
— Représente l'établissement lors des communications critiques en cas de crise cyber majeure

4.2.2. Responsable de la Sécurité des Systèmes d'Information (RSSI)

— Élabore et maintient à jour la PSSI et l'ensemble de la documentation sécurité
— Conseille la direction sur les risques et les mesures à prendre
— Coordonne les audits de sécurité et suit les plans de remédiation
— Pilote la réponse aux incidents de sécurité
— Rédige un rapport trimestriel et annuel sur l'état de la sécurité
— Établit et met à jour la cartographie des risques cyber (méthode EBIOS RM)
— Vérifie la conformité des projets aux exigences de sécurité (validation des DAT)
— Participe aux comités de projets impactant significativement le SI
— Définit et suit les indicateurs de performance sécurité (KPI et KRI)
— Anime le réseau des référents sécurité dans les services
— Développe et maintient les relations avec les autorités (ANSSI, CNIL, ARS)
— Supervise les tests d'intrusion et les exercices de cybersécurité
— Assure une veille active sur les menaces et vulnérabilités
— Collabore avec le DPO sur les aspects de protection des données personnelles
— Définit les plans de formation et sensibilisation à la cybersécurité

4.2.3. Délégué à la Protection des Données (DPO)

— Veille à la conformité des traitements au RGPD
— Tient le registre des traitements de données personnelles
— Évalue l'impact des nouveaux projets sur la protection des données
— Gère les demandes d'exercice de droits des patients

4.2.4. Direction des Systèmes d'Information (DSI)

— Implémente les mesures techniques de la PSSI
— Maintient l'infrastructure technique en conditions opérationnelles sécurisées
— Intègre les exigences de sécurité dans tous les projets informatiques
— Supervise les prestataires informatiques

4.2.5. Responsables des Services Médicaux et Administratifs

— Font appliquer la PSSI dans leurs services respectifs
— Signalent les incidents de sécurité constatés
— Participent à l'identification des besoins spécifiques de sécurité
— Sensibilisent leurs équipes aux bonnes pratiques

4.2.6. Utilisateurs

— Respectent les règles de sécurité énoncées dans la charte informatique
— Protègent leurs moyens d'accès (mots de passe, cartes)
— Signalent immédiatement tout incident de sécurité
— Participent aux formations de sensibilisation

4.3. Documentation de Sécurité

Notre architecture documentaire de sécurité s'organise hiérarchiquement :

1. **PSSI** : Document stratégique de référence (présent document)
2. **Politiques thématiques** :
   — Politique de gestion des identités et des accès
   — Politique de sécurité des données de santé
   — Politique de sécurité des équipements biomédicaux
3. **Procédures opérationnelles** :
   — Procédures de gestion des comptes utilisateurs
   — Procédures de sauvegarde et restauration

   - Procédures de gestion des incidents
4. **Instructions techniques** :
   - Instructions de durcissement des systèmes
   - Instructions de mise à jour des équipements
   - Instructions d'audit des logs

---

5. Mesures de Sécurité

5.1. Gestion des Identités et des Accès

5.1.1. Cycle de Vie des Identités

- Processus formalisé de création, modification et suppression des comptes :
  - Création des comptes uniquement par la DSI sur demande validée par la hiérarchie
  - Utilisation obligatoire du portail de gestion des identités pour toute demande
  - Workflow électronique de validation à double niveau pour les accès sensibles
  - Synchronisation automatique avec le SIRH (création automatisée à l'arrivée)
  - Convention de nommage uniforme : p.nom (première lettre du prénom + nom)
  - Attribution d'un matricule unique et permanent à chaque utilisateur
- Revue trimestrielle des droits d'accès aux applications critiques :
  - Extraction automatisée des droits affectés
  - Validation formelle par les responsables de service
  - Rapport d'anomalies généré et traité sous 10 jours ouvrés
  - Mesure du taux de comptes obsolètes ou incorrects
- Suppression automatique des accès après 90 jours d'inactivité :
  - Alerte automatique à J-15 de la désactivation
  - Processus de réactivation nécessitant validation hiérarchique
  - Archivage sécurisé des comptes désactivés pendant 1 an avant suppression définitive
- Révocation immédiate des droits lors des départs :
  - Intégration au processus de sortie des RH
  - Check-list de révocation multi-systèmes obligatoire
  - Confirmation de révocation complète sous 24h maximum
  - Audit mensuel des comptes associés à des personnes ayant quitté l'établissement

5.1.2. Authentification

- Authentification forte obligatoire pour les accès aux données de santé :
  - Carte CPS/CPE ou certificat électronique personnel
  - Code PIN ou mot de passe complexe
  - Biométrie pour les dispositifs mobiles institutionnels
- Politique de mot de passe conforme aux recommandations ANSSI :
  - Longueur minimale de 12 caractères
  - Complexité adaptée (majuscules, minuscules, chiffres, caractères spéciaux)
  - Renouvellement annuel obligatoire
  - Historique des 10 derniers mots de passe interdits à la réutilisation
- Blocage du compte après 5 tentatives infructueuses

5.1.3. Gestion des Droits d'Accès

- Attribution des privilèges selon le principe du moindre privilège
- Matrice des droits documentée et validée par les responsables métiers
- Procédure formelle de validation des demandes de droits exceptionnels
- Traçabilité de toutes les modifications de droits

5.1.4. Accès Privilégiés

- Séparation stricte des comptes administrateurs des comptes standards
- Double validation pour toute intervention sur les systèmes critiques
- Surveillance renforcée et analyse comportementale des comptes à privilèges élevés
- Coffre-fort numérique pour la gestion des identifiants privilégiés

5.2. Protection des Données

5.2.1. Classification et Traitement

- Classification formelle des données en 4 niveaux (public, interne, sensible, critique)
- Règles de traitement documentées pour chaque niveau de classification
- Inventaire des actifs de données critiques mis à jour semestriellement
- Étiquetage automatique des documents contenant des données sensibles

5.2.2. Chiffrement

- Chiffrement en transit :
  - TLS 1.2 minimum pour toutes les communications réseau
  - VPN obligatoire pour les accès distants
  - Protocoles sécurisés (HTTPS, SFTP) exclusivement
- Chiffrement au repos :
  - Chiffrement intégral des bases de données patient
  - Chiffrement des supports amovibles utilisés pour le transfert de données
  - Chiffrement des postes de travail et appareils mobiles

5.2.3. Anonymisation et Pseudonymisation

- Procédures d'anonymisation pour les données utilisées à des fins d'analyse
- Double clé de pseudonymisation pour les données de recherche
- Validation systématique des jeux de données avant extraction pour usage secondaire

5.2.4. Sauvegarde et Archivage

- Plan de sauvegarde différencié selon la criticité des données :
  - Données critiques : sauvegarde complète quotidienne, incrémentale toutes les 4 heures
  - Données sensibles : sauvegarde complète quotidienne, incrémentale quotidienne
  - Données internes : sauvegarde complète hebdomadaire, incrémentale quotidienne
- Tests de restauration mensuels documentés
- Archivage sécurisé conforme aux durées légales de conservation
- Site de réplication distant pour les données critiques (PRA)

5.3. Sécurité des Infrastructures

5.3.1. Sécurité Réseau

- Segmentation réseau par zones de sécurité :
  - Zone démilitarisée (DMZ) pour les services exposés :
    - Architecture multi-tiers avec pare-feu dédié
    - Serveurs reverse proxy avec WAF intégré
    - Inspection SSL/TLS des flux entrants
    - Hébergement des portails patients et partenaires
    - Limitation des services exposés au strict nécessaire (ports 80/443 uniquement)
  - Zone médicale pour les applications cliniques :
    - Isolation complète des réseaux contenant des données de santé
    - Accès conditionnel basé sur l'authentification et l'autorisation
    - Cloisonnement par type d'application (DPI, PACS, laboratoire, pharmacie)
    - Filtrage MAC pour les postes de travail dédiés
    - Surveillance comportementale en temps réel
  - Zone administrative pour les applications de gestion :
    - Segmentation par service (RH, comptabilité, logistique)
    - Restrictions des communications aux flux métiers légitimes
    - Contrôles d'accès stricts aux applications financières
    - Politiques de filtrage différenciées selon la sensibilité des données
  - Zone biomédicale pour les équipements connectés :
    - Isolation physique et logique du réseau biomédical
    - Contrôle d'accès basé sur les certificats d'équipement
    - Protection contre les interférences et perturbations
    - Monitoring continu des comportements anormaux

    - Systèmes anti-déni de service pour les équipements critiques
  - Zone IoT pour les objets connectés :
    - Réseau dédié et isolé pour tous les objets connectés non médicaux
    - Authentification mutuelle obligatoire pour tout nouvel équipement
    - Inspection profonde des paquets pour détecter les comportements anormaux
    - Restrictions de bande passante pour limiter l'impact des compromissions
- Filtrage des flux inter-zones par pare-feu de nouvelle génération :
  - Règles de filtrage basées sur les applications (Layer 7)
  - Inspection du contenu chiffré (SSL/TLS inspection)
  - Analyse comportementale des flux (détection d'anomalies)
  - Matrice de flux documentée et révisée trimestriellement
  - Validation des changements de règles via processus formel
  - Test et simulation avant déploiement des nouvelles règles
  - Rétention des logs de filtrage pendant 12 mois minimum
- Systèmes de détection/prévention d'intrusion (IDS/IPS) sur les segments critiques :
  - Déploiement en mode passif sur les zones standards (alertes)
  - Déploiement en mode actif sur les zones critiques (blocage)
  - Signatures actualisées quotidiennement
  - Règles personnalisées pour les applications métier spécifiques
  - Corrélation des alertes avec le SIEM central
  - Capacité de détection des attaques zero-day par analyse comportementale
- Contrôle des communications vers l'extérieur :
  - Proxy filtrant avec authentification obligatoire
  - Catégorisation des sites web et politique de filtrage différenciée
  - Analyse antimalware des fichiers téléchargés
  - Journalisation complète des accès externes
  - Blocage des catégories malveillantes et inappropriées
  - Inspection du contenu chiffré avec certificat institutionnel
- Analyse des flux réseau et détection d'anomalies (NDR) :
  - Sondes passives sur les points de concentration du réseau
  - Apprentissage des comportements normaux par IA
  - Détection des écarts statistiques significatifs
  - Identification des communications latérales suspectes
  - Découverte automatique des actifs non inventoriés
  - Visualisation des flux anormaux en temps réel

5.3.2. Sécurité des Serveurs et Systèmes

- Durcissement systématique selon les référentiels ANSSI et CIS
- Mise à jour mensuelle des correctifs de sécurité (critique sous 72h)
- Déploiement centralisé des configurations sécurisées
- Solution EDR (Endpoint Detection & Response) sur tous les serveurs critiques
- Gestion des vulnérabilités avec scan mensuel et plan de remédiation priorisé

5.3.3. Protection des Postes de Travail

- Solution de sécurité intégrée :
  - Antivirus/antimalware avec mise à jour quotidienne
  - Filtrage des sites malveillants
  - Contrôle des applications autorisées (whitelisting)
- Verrouillage automatique après 10 minutes d'inactivité
- Restriction des droits d'installation de logiciels
- Mécanisme de filtrage USB et contrôle des périphériques
- Chiffrement intégral des disques

5.3.4. Sécurité des Dispositifs Médicaux Connectés

- Inventaire exhaustif de tous les équipements biomédicaux connectés
- Réseau isolé dédié avec surveillance spécifique
- Procédure de qualification de sécurité avant mise en production
- Plan de maintenance de sécurité coordonné avec le service biomédical
- Protection spécifique contre les interférences électromagnétiques malveillantes

5.4. Gestion des Incidents de Sécurité

5.4.1. Détection et Signalement

- Centre opérationnel de sécurité (SOC) pour la surveillance 24/7
- Procédure de signalement accessible à tous les utilisateurs
- Canaux d'alerte multiples (téléphone hotline, portail intranet, email dédié)
- Remontée automatisée des alertes techniques critiques
- Programme de récompense pour le signalement des vulnérabilités

5.4.2. Qualification et Traitement

- Échelle de gravité des incidents formalisée (4 niveaux)
- Procédures de réponse adaptées à chaque typologie d'incident
- Équipe de réponse aux incidents de sécurité (CSIRT) avec astreinte
- Isolation automatique des systèmes compromis
- Coordination avec les autorités compétentes (ANSSI, CNIL, ARS)

5.4.3. Investigation et Analyse

- Outils de forensique numérique pour analyse des compromissions
- Procédures de collecte de preuves numériques
- Analyse des causes profondes après résolution
- Conservation sécurisée des éléments de preuves

5.4.4. Communication de Crise

- Procédure de communication interne et externe
- Modèles de communication préétablis
- Formation des porte-paroles aux situations de crise cyber
- Coordination obligatoire avec la Direction et les relations publiques

---

6. Sensibilisation et Formation

6.1. Programme de Sensibilisation

6.1.1. Actions Générales

- Campagne annuelle de sensibilisation à la sécurité :
  - Semaine de la cybersécurité hospitalière (ateliers pratiques)
  - Conférences par des experts externes et retours d'expérience
  - Sessions de démonstration des attaques courantes
  - Challenge inter-services sur les bonnes pratiques
  - Évaluation de l'impact par questionnaire avant/après
  - Remise de matériel de sensibilisation (mémo-cartes, guide pratique)
- Communications mensuelles sur les menaces actuelles :
  - Alerte rapide sur les nouvelles cybermenaces ciblant le secteur santé
  - Cas pratiques issus d'incidents réels (anonymisés)
  - Conseils personnalisés selon les profils utilisateurs
  - Diffusion multicanale (intranet, email, affichage, écrans d'information)
  - Code couleur d'alerte selon le niveau de risque (vert, orange, rouge)
- Affichage des bonnes pratiques dans les espaces communs :
  - Infographies pédagogiques dans les salles informatiques
  - Affiches thématiques rotatives (mot de passe, phishing, dispositifs mobiles)
  - QR codes renvoyant vers des ressources détaillées
  - Messages clés sur les écrans de veille des postes de travail
  - Pictogrammes standardisés pour faciliter la mémorisation
- Newsletter trimestrielle dédiée à la cybersécurité :
  - Revue des incidents récents et mesures prises
  - Témoignages d'utilisateurs et retours d'expérience
  - Innovations en matière de sécurité déployées dans l'établissement
  - Interview d'un expert par numéro

    - Rubrique FAQ répondant aux questions fréquentes des utilisateurs
    - Format numérique interactif avec quizz intégré
- Rappels automatiques des règles clés lors de la connexion :
    - Messages contextuels selon le profil utilisateur et l'application
    - Rotation des messages de sensibilisation (banque de 20 messages)
    - Validation de lecture obligatoire pour les alertes importantes
    - Conseils personnalisés basés sur les comportements observés
    - Mini-tutoriels interactifs lors des premières utilisations de nouveaux services

6.1.2. Actions Ciblées

- Sensibilisation spécifique pour les nouveaux arrivants (intégrée à l'onboarding)
- Sessions adaptées aux profils métiers (médecins, administratifs, techniques)
- Exercices périodiques de phishing simulé avec retour personnalisé
- Ateliers pratiques sur des cas réels d'incidents

6.2. Formation

6.2.1. Formation des Utilisateurs

- Formation initiale obligatoire à la sécurité pour tout nouvel arrivant
- Formation continue annuelle avec validation des connaissances
- Modules e-learning thématiques (protection du mot de passe, phishing, etc.)
- Formation approfondie pour les référents sécurité des services

6.2.2. Formation des Équipes Techniques

- Plan de formation certifiant pour l'équipe sécurité
- Formations spécifiques sur les technologies déployées
- Participation aux conférences et événements sectoriels
- Exercices pratiques de gestion d'incidents (Red Team/Blue Team)

6.2.3. Formation des Managers

- Sensibilisation spécifique aux responsabilités légales
- Formation à la gestion des incidents et des crises
- Intégration de la sécurité dans les processus décisionnels
- Méthodes d'évaluation des risques cyber

6.3. Évaluation et Suivi

- Tests de connaissances après chaque session de formation
- Indicateurs de performance (taux de réussite, participation)
- Enquêtes de perception de la sécurité
- Analyse de l'efficacité (corrélation avec les incidents)

---

7. Audit et Contrôle

7.1. Programme d'Audit

7.1.1. Audits Internes

- Programme annuel d'audits internes couvrant l'ensemble des domaines de la PSSI
- Audits spécifiques lors de changements majeurs du SI
- Auto-évaluation annuelle des services (matrice de maturité)
- Revue des droits d'accès trimestrielle

7.1.2. Audits Externes

- Audit complet de sécurité externe annuel
- Tests d'intrusion semestriels (externe et interne)
- Scan de vulnérabilités trimestriel par prestataire qualifié
- Audit de certification HDS tous les 3 ans

7.1.3. Méthodes et Référentiels

- Audits basés sur les référentiels ISO 27001, HDS et RGPD
- Méthodologie EBIOS Risk Manager pour les analyses de risque
- Framework NIST pour l'évaluation de la maturité cybersécurité
- Guide d'hygiène informatique de l'ANSSI pour les contrôles basiques

7.2. Contrôles Techniques Permanents

- Surveillance continue des événements de sécurité (SIEM)
- Analyse automatisée des configurations (conformité)
- Scan hebdomadaire des vulnérabilités techniques
- Surveillance des comportements anormaux (UEBA)
- Tests automatisés des contrôles de sécurité critiques

7.3. Reporting et Amélioration

- Tableau de bord mensuel des indicateurs de sécurité
- Rapport trimestriel au comité de sécurité
- Rapport annuel consolidé à la Direction
- Suivi des plans d'action correctifs et préventifs
- Mesure des niveaux de maturité par domaine

---

8. Mise à Jour et Amélioration Continue

8.1. Cycle de Révision

- Révision complète de la PSSI tous les 2 ans :
  - Processus structuré démarrant 6 mois avant l'échéance
  - Constitution d'un groupe de travail pluridisciplinaire
  - Évaluation de l'applicabilité et de l'efficacité de chaque mesure
  - Benchmark avec d'autres établissements de santé (minimum 3)
  - Consultation des référents métiers de chaque service
  - Prise en compte des audits et tests réalisés sur la période
  - Mise à jour de l'analyse des risques (EBIOS RM)
  - Validation progressive (RSSI → Comité de sécurité → Direction)
  - Communication formelle après approbation
  - Conservation des versions historiques pour traçabilité
- Mise à jour des annexes techniques annuellement :
  - Revue systématique de chaque annexe avec les experts techniques
  - Intégration des évolutions technologiques significatives
  - Mise à jour des configurations de référence
  - Actualisation des listes de contrôle et procédures opérationnelles
  - Ajustement des indicateurs de performance
  - Mise en cohérence avec les évolutions de l'infrastructure
  - Processus léger de validation (RSSI + DSI)
- Révision extraordinaire après un incident majeur :
  - Déclenchement automatique pour tout incident de niveau 1 ou 2
  - Analyse ciblée des sections concernées par l'incident
  - Intégration des enseignements de la gestion de crise
  - Renforcement des mesures défaillantes identifiées
  - Validation accélérée des modifications critiques
  - Communication spécifique sur les changements apportés
- Revue de cohérence après chaque évolution réglementaire significative :
  - Analyse d'impact par le service juridique et le RSSI
  - Identification des sections et mesures impactées
  - Rédaction des modifications nécessaires
  - Mise en conformité dans les délais imposés par la réglementation
  - Documentation des changements dans un registre dédié
  - Traçabilité des versions pour démontrer la conformité

8.2. Veille et Anticipation

8.2.1. Veille Technologique

— Suivi des évolutions technologiques impactant la sécurité
— Abonnement aux bulletins de sécurité éditeurs
— Participation aux groupes d'échange sectoriels
— Benchmark des pratiques dans le secteur hospitalier

8.2.2. Veille sur les Menaces

— Abonnement aux alertes CERT-FR et CERT Santé
— Intégration au réseau national de cybersurveillance santé
— Analyse des cyberattaques touchant le secteur de la santé
— Mise à jour des scénarios de menace selon l'évolution du contexte

8.3. Gestion des Evolutions

— Processus d'évaluation de l'impact sécurité des changements (Security Impact Assessment)
— Comité d'architecture de sécurité pour validation des évolutions majeures
— Tests de sécurité systématiques avant déploiement (DevSecOps)
— Période de surveillance renforcée après changement significatif

---

9. Conformité Réglementaire

9.1. Cadre Réglementaire Applicable

— Règlement Général sur la Protection des Données (RGPD)
— Certification Hébergeur de Données de Santé (HDS)
— Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)
— Code de la Santé Publique
— Directive NIS2 et sa transposition nationale
— Loi de Programmation Militaire (articles relatifs aux OIV)

9.2. Mécanismes de Conformité

9.2.1. Protection des Données Personnelles

— Analyses d'impact relatives à la protection des données (AIPD) pour tous les traitements sensibles
— Registre des traitements mis à jour trimestriellement
— Procédures d'exercice des droits des personnes concernées
— Encadrement des transferts de données hors UE

9.2.2. Hébergement des Données de Santé

— Certification HDS pour les systèmes concernés
— Contrats conformes avec les sous-traitants hébergeurs
— Audits réguliers des conditions d'hébergement
— Plan de réversibilité documenté

9.2.3. Traçabilité et Imputabilité

— Conservation des traces pendant les durées légales
— Horodatage qualifié des événements critiques
— Mécanismes d'intégrité des journaux d'événements
— Procédures de mise à disposition aux autorités compétentes

9.3. Relations avec les Autorités

— Point de contact désigné pour les relations avec la CNIL
— Procédure de notification des violations de données (72h)
— Coordination avec l'ANSSI en cas d'incident majeur
— Reporting régulier à l'ARS sur l'état de la sécurité numérique

10. Gestion de Crise

10.1. Préparation

- Plan de gestion de crise cyber formalisé et validé par la Direction
- Cellule de crise cybersécurité identifiée avec rôles prédéfinis
- Scénarios de crise documentés pour les principales menaces
- Coordination établie avec le plan blanc de l'établissement
- Ressources techniques et humaines identifiées et mobilisables

10.2. Organisation et Gouvernance de Crise

- Structure décisionnelle à trois niveaux :
  - Niveau stratégique : Direction générale et RSSI
  - Niveau tactique : Responsables de services impactés
  - Niveau opérationnel : Équipes techniques d'intervention
- Locaux de crise équipés et sécurisés
- Moyens de communication alternatifs (indépendants du SI principal)
- Procédures de remontée d'information et de reporting

10.3. Plans de Continuité et de Reprise

- Plan de Continuité d'Activité (PCA) détaillant :
  - Processus métiers critiques et leurs dépendances IT :
    - Classification des processus par niveau de criticité (P0 à P3)
    - Cartographie des dépendances applicatives et techniques
    - Identification des ressources minimales requises par processus
    - Définition des impacts métier acceptables (DMIA/RTO/RPO)
    - Matrice de corrélation processus métiers / composants techniques
    - Évaluation de la criticité temporelle (impacts à H+1, H+4, H+24...)
  - Procédures manuelles de substitution :
    - Modes dégradés documentés pour chaque application critique
    - Formulaires papier standardisés pré-imprimés et stockés
    - Procédures détaillées par service et par fonction
    - Documentation accessible hors système d'information
    - Formation régulière du personnel aux modes dégradés (2 fois/an)
    - Rotations organisées pour maintenir les compétences
    - Chaîne logistique pour la distribution des supports papier
    - Procédures de ressaisie post-incident
  - Seuils de déclenchement et chaîne d'escalade :
    - Définition précise des critères de déclenchement
    - Niveaux progressifs d'activation (veille, préalerte, activation)
    - Autorités de décision identifiées par niveau et par plage horaire
    - Procédures de communication interne et externe prédéfinies
    - Canaux de communication alternatifs (téléphonie dédiée)
    - Points de situation standardisés (fréquence et format)
    - Règles de passage d'un niveau à l'autre (escalade/désescalade)
  - Priorisation des systèmes à maintenir :
    - Classification par priorité de reprise (1 à 4)
    - Focus prioritaire sur les systèmes liés aux soins vitaux
    - Identification des interdépendances techniques
    - Séquencement optimal de reprise documenté
    - Allocation prévisionnelle des ressources techniques
    - Validation médicale de la priorisation des systèmes
    - Révision semestrielle de la hiérarchisation
- Plan de Reprise d'Activité (PRA) couvrant :
  - Architecture technique de secours :
    - Site de reprise distant (>30km) avec infrastructure redondante
    - Capacité de reprise à 50% minimum des systèmes critiques
    - Lien télécom diversifié et sécurisé entre sites principal et secours

    - Synchronisation des données en temps réel pour les systèmes critiques
    - Infrastructure externalisée chez un prestataire HDS certifié
    - Solutions cloud sécurisées pour certaines applications
    - Systèmes énergétiques autonomes (groupe électrogène + onduleurs)
    - Accès physique sécurisé avec procédures d'urgence
  - Procédures de bascule et de restauration :
    - Check-lists détaillées par système et application
    - Rôles et responsabilités précisément définis
    - Workflows documentés avec points de validation
    - Scripts automatisés de bascule et validation
    - Procédures de vérification d'intégrité des données
    - Mécanismes de synchronisation post-reprise
    - Documentation des configurations réseau alternatives
    - Procédures de basculement réseau (DNS, load-balancing)
  - Séquence de redémarrage des systèmes :
    - Ordonnancement précis documenté par dépendances
    - Diagramme de Gantt détaillant les étapes et durées estimées
    - Points de contrôle obligatoires avant progression
    - Validation des prérequis techniques à chaque étape
    - Tests d'intégrité applicative intégrés au processus
    - Validation fonctionnelle par les référents métiers
    - Procédures de rollback à chaque étape en cas d'échec
    - Évaluation temps réel de la progression
  - Tests de reprise programmés semestriellement :
    - Alternance entre tests partiels et tests complets
    - Scénarios variés à chaque exercice (causes différentes)
    - Implication des utilisateurs clés dans les tests
    - Mesure précise des temps de reprise réels
    - Rapports détaillés d'anomalies et d'amélioration
    - Suivi des KPI de reprise (taux de réussite, délais)
    - Tests inopinés annuels avec périmètre limité
    - Rotation des équipes impliquées pour diffuser les compétences

10.4. Gestion Post-Crise

- Procédures de retour à la normale
- Analyse post-incident (RETEX)
- Plan d'amélioration suite aux enseignements
- Communication de clôture de crise

---

11. Annexes Techniques

11.1. Exigences Minimales de Sécurité

- Liste des configurations de sécurité minimales par type d'équipement :
  - **Postes de travail** :
    - Protection antimalware avec mise à jour quotidienne automatique
    - Chiffrement intégral du disque (BitLocker/LUKS)
    - Pare-feu local activé et configuré
    - Déploiement centralisé des mises à jour de sécurité (délai max : critique 72h, autres 30j)
    - Désactivation des ports USB non autorisés
    - Écran de verrouillage automatique après 10 minutes d'inactivité
    - Désactivation des services et protocoles non essentiels
    - Inventaire automatisé des logiciels installés
    - Application des GPO de sécurité institutionnelles
    - Comptes utilisateurs sans droits d'administration
    - Journalisation centralisée des événements de sécurité
    - Solution EDR avec détection comportementale
  - **Serveurs** :
    - Installation minimale (hardening) selon référentiels CIS

  - Mises à jour de sécurité déployées sous 72h pour correctifs critiques
  - Authentification forte pour tous les accès administrateurs
  - Séparation des rôles et privilèges par serveur
  - Règles de pare-feu restrictives (défaut : tout bloquer)
  - Journalisation avancée et remontée au SIEM central
  - Surveillance des modifications de fichiers critiques (FIM)
  - Protection antimalware avec exclusions documentées
  - Chiffrement des volumes de données sensibles
  - Supervision complète (disponibilité, performance, sécurité)
  - Sauvegardes chiffrées et testées régulièrement
  - Désactivation des comptes par défaut ou changement systématique
  - Protection contre les attaques par force brute
  - Isolation des services sur des VLAN dédiés
  - Bannière d'avertissement légal à la connexion
- **Équipements réseau** :
  - Changement systématique des identifiants par défaut
  - Restriction des interfaces de gestion (ACL IP)
  - Chiffrement de toutes les communications d'administration (SSH/HTTPS)
  - Authentification RADIUS ou TACACS+ pour les administrateurs
  - Filtrage MAC sur les ports d'accès
  - Désactivation des protocoles obsolètes (telnet, SNMPv1/v2)
  - Utilisation de SNMPv3 avec authentification et chiffrement
  - Synchronisation NTP avec source fiable
  - Journalisation des connexions et modifications
  - Sauvegarde chiffrée des configurations
  - Mise à jour du firmware selon recommandations constructeur
  - Désactivation des services et ports inutilisés
  - Protection contre les attaques DoS/DDoS sur équipements exposés
  - Redondance physique pour les équipements critiques
  - Surveillance des performances et de la sécurité
- **Périphériques mobiles** :
  - Inscription obligatoire dans la solution MDM institutionnelle
  - Chiffrement intégral du stockage
  - Code PIN ou biométrie obligatoire (pas de schéma)
  - Effacement à distance activé
  - Limitation des applications installables (whitelist)
  - VPN obligatoire pour l'accès aux ressources internes
  - Mise à jour automatique du système d'exploitation
  - Conteneurisation des données professionnelles
  - Désactivation des services de localisation non essentiels
  - Politique de verrouillage automatique après 5 minutes
  - Suppression automatique après 10 tentatives incorrectes
  - Filtrage web en mobilité
  - Antimalware pour appareils Android
  - Désactivation du jailbreak/root
  - Configurations WiFi sécurisées préinstallées
- **Dispositifs médicaux connectés** :
  - Inventaire détaillé et mise à jour continue
  - Séparation réseau dédiée
  - Protection contre modification non autorisée
  - Durcissement selon recommandations fabricant
  - Suppression des comptes par défaut
  - Authentification forte pour la maintenance
  - Mise à jour selon processus validé par biomédical
  - Surveillance des communications réseau
  - Chiffrement des données transmises
  - Audit de sécurité avant mise en production
  - Documentation de toutes les interventions
  - Protection physique des interfaces sensibles
  - Désactivation des services non utilisés
  - Filtrage des flux entrants/sortants

  - Liaison avec le SIEM si possible
- Exigences techniques pour les nouveaux projets :
  - Analyse de risque obligatoire en phase avant-projet
  - Cahier des charges incluant annexe sécurité détaillée
  - Clauses contractuelles de sécurité pour les fournisseurs
  - Validation architecturale par l'équipe sécurité avant déploiement
  - Tests de sécurité obligatoires avant mise en production
  - Livraison du code source quand applicable
  - Garanties de maintenance sécurité pendant toute la durée de vie
  - Documentation technique complète des mesures de sécurité
  - Plan de gestion des vulnérabilités
  - Plan de réversibilité ou de fin de vie
  - Intégration avec le système d'authentification central
  - Compatibilité avec les solutions de sauvegarde institutionnelles
  - Génération de journaux au format standard
  - Formation sécurité pour les administrateurs et utilisateurs
  - Procédures de reprise d'activité documentées

11.2. Procédures Opérationnelles

- Procédures de gestion des comptes et des accès
- Procédures de sauvegarde et restauration
- Procédures de mise à jour de sécurité
- Procédures de gestion des vulnérabilités

11.3. Cartographie des Risques

- Matrice des risques cyber majeurs
- Cartographie des flux d'information critiques
- Matrice de dépendances entre systèmes
- Plan de traitement des risques priorisé

11.4. Indicateurs de Performance

- Tableau de bord SSI avec indicateurs clés
- Seuils d'alerte pour chaque indicateur
- Méthodologie de mesure et de collecte
- Exemple de rapport périodique

---

12. Conclusion

Cette Politique de Sécurité des Systèmes d'Information détaillée constitue l'engagement formel de notre établissement hospitalier à protéger son patrimoine informationnel, à garantir la continuité des soins et à préserver la confiance des patients. L'application rigoureuse de ces directives par l'ensemble des acteurs est essentielle pour faire face aux menaces cyber croissantes ciblant le secteur de la santé.

La PSSI sera adaptée en permanence pour répondre aux évolutions technologiques, réglementaires et aux nouvelles menaces. La sécurité étant l'affaire de tous, chaque collaborateur est un maillon essentiel de notre chaîne de protection.