|  |
| --- |
|  |
| PSSI |
| CHU de Ynov |

|  |
| --- |
| VIOLLET Yoan, ETESSE Tristan |

# 1. Introduction

Le Centre Hospitalier Universitaire (CHU) de Ynov utilise de nombreuses ressources informatiques pour assurer la continuité et la qualité des soins. Cette Politique de Sécurité des Systèmes d’Information (PSSI) vise à protéger les actifs numériques de l’établissement, garantir la confidentialité des données patients, et assurer la disponibilité des services critiques.

# 2. Périmètre de la PSSI

Cette politique couvre l’ensemble du système d’information du CHU de Ynov, incluant :  
- Le réseau segmenté par VLANs (médical, administratif, invités, management)  
- Les serveurs et applications critiques (Web, BDD, AD, DNS, DHCP)  
- Les dispositifs médicaux connectés  
- Les postes clients  
- Les équipements réseau et l’infrastructure de virtualisation  
- Les utilisateurs internes (médicaux, administratifs, IT)

# 3. Objectifs de sécurité

Les trois objectifs fondamentaux sont :  
- Confidentialité : garantir la protection des données personnelles et médicales  
- Intégrité : assurer la fiabilité des informations échangées  
- Disponibilité : garantir l’accès aux systèmes vitaux à tout moment

# 4. Gouvernance et responsabilités

La responsabilité de la sécurité du SI incombe à la Direction Informatique. Les tâches sont réparties comme suit :  
- RSSI : supervision de la sécurité globale et des incidents  
- Administrateurs systèmes : mise en œuvre des configurations sécurisées  
- Utilisateurs : respect des bonnes pratiques de cybersécurité définies

# 5. Classification des actifs

Les actifs sont classés par criticité :  
- Critiques : dossiers médicaux, serveurs applicatifs, systèmes de soins  
- Importants : outils administratifs, AD, DNS, systèmes RH  
- Modérés : postes utilisateurs, réseau invité

# 6. Mesures organisationnelles

- Attribution de rôles selon le principe du moindre privilège  
- Accès différencié entre les VLANs via des ACLs  
- Mise en œuvre d’un bastion d’administration  
- Formation initiale à la sécurité pour tout nouveau personnel  
- Procédures d’escalade en cas d’incident

# 7. Mesures techniques

- Segmentation réseau en VLANs avec filtrage ACLs  
- IDS Snort sur VLAN management pour la détection d’intrusion  
- Pare-feu pfSense à configurer pour les flux inter-VLAN  
- Mise à jour régulière des OS et services critiques  
- Journalisation des événements sur un serveur central (prévu via SIEM)

# 8. Gestion des accès

- Authentification locale ou via Active Directory  
- MFA pour les comptes à privilèges  
- Politique de mot de passe : minimum 12 caractères, complexité imposée, changement tous les 90 jours  
- Suppression immédiate des comptes obsolètes

# 9. Sauvegardes et plan de continuité

- Sauvegardes chiffrées quotidiennes des bases critiques, hebdomadaires complètes  
- Stockage des sauvegardes sur serveur distant ou support externe  
- Plan de reprise (PRA) : redéploiement des VMs critiques en 2h via snapshots  
- Plan de continuité (PCA) : maintien de l’accès aux services essentiels même en mode dégradé

# 10. Sensibilisation du personnel

- Présentation annuelle sur les menaces courantes : phishing, ransomware  
- Affiches de sensibilisation dans les locaux  
- Simulations d’attaque organisées par l’équipe IT  
- Fiches réflexes en cas de suspicion d’incident

# 11. Surveillance et gestion des incidents

- Mise en place d’un SIEM (ex. : ELK/Splunk) pour corrélation des logs (en projet)  
- Journalisation centralisée  
- Procédure d’analyse d’incident et réponse en moins de 4h  
- Tests d’intrusion trimestriels (internes ou simulés)

# 12. Conformité réglementaire

Le CHU de Ynov s’engage à :  
- Respecter le RGPD pour la gestion des données à caractère personnel  
- Se conformer aux bonnes pratiques de la norme ISO 27001  
- Définir un registre des traitements de données sensibles

# 13. Évolution de la politique

Cette politique est revue chaque année par la Direction Informatique. Elle peut être modifiée suite à :  
- Un audit  
- Un incident majeur  
- Une évolution technologique ou réglementaire