

	Manuel GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	Plan d'Assurance Sécurité	Référence :	SI-ORG-MANG-001
		Date de création :	10/01/2024
		Page :	Page 1 sur 4
		Version :	1

	Rédaction	Forme vérifiée par DQGDR	Validation
Nom	PETIT Virginie	PETIT Virginie (18/03/2025)	LENGLET William (18/03/2025)

Type de diffusion : Interne

Sommaire	
Table des matières	
1. Objet du document	1
2. Description des exigences de sécurité	1
2.1. Politiques de sécurité de l'information.	1
2.2. Organisation de la sécurité de l'information	2
2.3. Gestion des actifs	2
2.4. Sécurité liée aux ressources humaines	2
2.5. Sécurité physique et environnementale	2
2.6. Gestion de l'exploitation et des télécommunications	3
2.6.1. Gestion de l'exploitation	3
2.6.2. Sécurité des communications	3
2.7. Maîtrise des accès logiques	3
2.8. Gestion des incidents de sécurité	4
2.9. Gestion du Plan de continuité d'activité	4
2.10. Conformité	4

1. Objet du document

Le plan d'Assurance de Sécurité de l'Information (PAS) rassemble tous les contrôles de sécurité et des services de sécurité définis et mis en place par le CHU pour assurer le bon niveau de sécurité des activités qu'il réalise dans le cadre de l'hébergement des données des établissement du Groupement Hospitalier Universitaire de Champagne (GHUC).

2. Description des exigences de sécurité

2.1. Politiques de sécurité de l'information.

	Manuel GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	Plan d'Assurance Sécurité	Référence :	SI-ORG-MANG-001
		Date de création :	10/01/2024
		Page :	Page 2 sur 4
		Version :	1

La PGSSI (Politique Générale de Sécurité des Systèmes d'Informations) est formalisée et appliquée.

Notre PGSSI et les politiques thématiques et opérationnelle respectent les lois et les réglementations, elles sont régulièrement revues et mises à jour.

2.2. Organisation de la sécurité de l'information

Un Responsable de la Sécurité des Systèmes d'Information est nommé et prend en charge la sécurité des interventions et de l'opération des outils de sécurité des données hébergées sur notre établissement.

Une Déléguée à la Protection des Données (DPD) est nommée et, est en charge du respect de la réglementation concernant la sécurité et la protection des données.

La Cellule Qualité & Sécurité (CQS) transmet aux établissements partenaires les informations, requêtes ou certificats des autorités (CERT-FR, CERT-Santé, ARS...)

Le RSSI et la CQS définissent et font respecter des règles relatives à la protection des informations (copie, diffusion, conservation, destruction, transmission).

2.3. Gestion des actifs

Le RSSI et la CQS définissent et font appliquer aux informations et actifs hébergés par le CHU des règles de classification et de marquage respectant l'exigence de la norme ISO27001.

2.4. Sécurité liée aux ressources humaines

La Direction des Services Numériques (DSN) et les responsables de secteurs sont responsables de la sélection de ses employés et des sous-traitants qui interviennent sur l'environnement hébergé du CHU.

Les termes et conditions d'embauche incluent des obligations contractuelles de sécurité de l'information dans les contrats de tous les employés ou sous-traitants qui interviennent sur l'environnement hébergé du CHU (confidentialité, accords de non divulgation, respect de la propriété intellectuelle, etc.)

La DSN, plus spécifiquement la CQS, informe et sensibilise les personnels intervenants sur l'environnement hébergé du CHU aux règles de sécurité spécifiques.

2.5. Sécurité physique et environnementale

Le RSSI et la CQS définissent, implémentent et revoient les mesures de sécurisation des zones, ils mettent en place des mesures de protection des locaux.

Ils mettent en place et revoient les mesures liées à la sécurisation des matériels.

Ils exécutent l'ensemble des activités sur l'environnement hébergé du CHU depuis les locaux de la DSN.

	Manuel GHUC		
	Groupeement Hospitalier Universitaire de Champagne		
	Plan d'Assurance Sécurité	Référence :	SI-ORG-MANG-001
		Date de création :	10/01/2024
		Page :	Page 3 sur 4
		Version :	1

2.6. Gestion de l'exploitation et des télécommunications

2.6.1. Gestion de l'exploitation

Le CHU de Reims s'engage à documenter et maintenir des procédures dans le cadre de l'hébergement de l'environnement des établissements partenaires.

Le CHU de Reims mettra en œuvre le processus de gestion des changements, à savoir :

- Identifier et appliquer les mesures de sécurité dans le processus de gestion des changements
- Conserver les traces de tous les changements
- Planifier en accord avec l'établissement partenaire
- Evaluer les impacts potentiels des changements
- Définir les procédures de communication

La sauvegarde des informations est formellement formalisée dans la politique de sauvegarde du CHU de Reims

Le CHU de Reims maintient une solution de sauvegarde et de restauration de l'environnement hébergé conformément aux besoins de l'établissement partenaire. Il teste la solution sauvegarde/restauration.

La prise de main à distance d'une ressource informatique n'est réalisée que par des personnes autorisées. Ils mettent en place et font respecter des mesures de sécurité spécifiques à la prise de main à distance. Il s'assure que les comptes de service font l'objet d'une restriction de droits en suivant le principe du moindre privilège via la gestion et l'installation des logiciels en exploitation sont définies par des restrictions d'installation.

2.6.2. Sécurité des communications

Suivant sa politique de cloisonnement, le CHU de Reims implémente des zones cloisonnées pour les établissements partenaires

Le CHU de Reims est responsable des équipements réseau et des liaisons de télécommunications (routeurs, switches, firewalls...).

Le CHU de Reims se soumet à une politique de gestion des actifs et transfert de données, Dès que les médias physiques sont utilisés pour le transfert de l'information, l'établissement partenaire devra mettre en place des mesures pour enregistrer les médias physiques contenant des données personnelles entrants et sortants.

Aussi, le CHU de Reims propose l'utilisation de Owncloud et de Nextcloud pour le transfert et la protection des informations sensibles.

2.7. Maîtrise des accès logiques

Le CHU de Reims met en place des mesures de contrôle d'accès du personnel sur les systèmes (identification et authentification, mise en veille et déconnexion automatiques, séparation des tâches, gestion des droits, traçabilité des actions).

Il met en œuvre des mesures de sécurité (liaison VPN SSL avec authentification du personnel, accès uniquement avec un ordinateur sécurisé) pour les interventions à distance de ses personnels

	Manuel GHUC		
	Groupeement Hospitalier Universitaire de Champagne		
	Plan d'Assurance Sécurité	Référence :	SI-ORG-MANG-001
		Date de création :	10/01/2024
		Page :	Page 4 sur 4
		Version :	1

2.8. Gestion des incidents de sécurité

L'établissement partenaire informera le RSSI du GHT de tout incident de sécurité.

Les incidents de sécurité, selon la procédure de gestion des incidents graves en place et selon sa PGSSI, seront gérés conjointement avec l'établissement partenaire.

La cellule de crise prendra les mesures nécessaires pour veiller à ce que tels incidents ne se reproduisent pas.

Le CHU de Reims assurera une assistance, en cas de besoin, pour permettre l'analyse et la collecte de preuves.

2.9. Gestion du Plan de continuité d'activité

La continuité et la gestion des mesures relatives à la sécurité de l'information incombe au CHU de Reims. Il avisera l'établissement partenaire avant de mener les tests de la continuité d'activité

2.10. Conformité

- Le CHU de Reims s'engage à :
- Définir et documenter les mesures spécifiques et les responsabilités pour être en conformité avec les lois et règlements applicables
- Effectuer une revue de la sécurité de l'information via des audits réguliers
- Effectuer une analyse d'écarts entre la PGSSI et le niveau de la sécurité de l'établissement partenaire
- Évaluer les risques et les plans de correction.
- Initier le processus de gestion du changement pour les mesures de correction nécessaires, et les implémenter les actions de correction.
- Planifier et documenter les tests d'intrusion et de recherche de vulnérabilité sur leur périmètre de responsabilité
- Définir des procédures, des outils et des exigences techniques
- Mettre en place la gestion de la conformité des systèmes par rapport à la PGSSI