	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 1 sur 16
		Version	V2.0

Sommaire


1	Introduction	2
1.1	Contexte	2
1.2	Objectifs	2
1.3	Périmètre d'application	2
2	Exigences	3
2.1	Cartographie	4
2.2	Protection des données	5
2.3	Protection des actifs	5
2.4	Transfert de données.....	6
2.5	Mise au rebut.....	8
2.6	Transfert physique des supports	9
2.7	Réglementaire	10
2.8	Vol et perte de matériel	10
3	Annexe.....	11
3.1	Glossaire.....	11
3.2	Références	11
3.3	RACI	12
3.4	Revue de la politique	12
3.5	Grille de classification DICT	13
3.6	Mesures de sécurité	14

Version	Date d'actualisation	Modifications apportées (page / contenu)
V0.1	22/07/2022	Création du document
V1.1	11/10/2022	Validation du COSSI
V1.2	02/10/2023	Revue COSSI
V2.0	30/09/2024	Ajout acronymes dans le glossaire et ajout classification du document. Validation COSSI du 01/10/2024

	Rédaction	Validation
Nom	Thomas Virginie	COSSI
Date	22/07/2022	11/10/2022

Classification du document

Interne

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 2 sur 16
		Version	V2.0

1 Introduction

1.1 Contexte

Le Système de Management de la Sécurité de l'Information (SMSI) permet de mettre en œuvre une démarche ayant pour but de maîtriser la Sécurité du Système d'Information du CHU de Reims.

Dans le cadre de leur activité, les collaborateurs et prestataires du CHU de Reims sont amenés à manipuler des actifs (tant matériel qu'immatériel, à savoir des données) dont la confidentialité, l'intégrité ou la disponibilité peuvent avoir un caractère essentiel.

Pour offrir une protection adéquate, il est important d'évaluer les impacts qu'aurait une perte de confidentialité, d'intégrité ou de disponibilité de ces derniers. Cette évaluation, appelée classification SSI, se doit d'être basée sur des critères objectifs afin d'être répétable dans le temps.

1.2 Objectifs


Les objectifs de cette politique sont :

- Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée ;
- S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à sa sensibilité pour le CHU de Reims ;
- Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation qu'elle soit stockée sur des supports ou en mouvement ;
- Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

1.3 Périmètre d'application

Les exigences concernent l'ensemble des acteurs du CHU de Reims, qu'ils soient internes ou externes, et notamment :

- Le RSSI ;
- Le DPD ;
- Les responsables métier ;
- Les chefs de projets SI ;
- Les utilisateurs ;
- Les administrateurs ;
- Les prestataires de service.

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 3 sur 16
		Version	V2.0

2 Exigences

Les exigences ci-après prennent la forme d'un marquage précis : **EO-FOU-X** ou **EC-FOU-X**.

Les **E**xigences sont **O**bligatoires : **EO**, ou **C**onseillées : **EC**.

Une exigence est obligatoire lorsque :


- Elle constitue une exigence légale et/ou réglementaire (ex : exigences contractuelles, RGPD) ;
- Elle constitue une exigence de la norme ISO 27001 et de son annexe A ;
- Son application est fondamentale pour la sécurité du système d'information du CHU de Reims.

Une exigence est conseillée lorsque :

- Elle constitue une bonne pratique ;
- Son application rentre dans une démarche d'amélioration continue.

Index :


EO-ACT-01 : Inventaire	EC-ACT-11 : Besoin d'en connaître
EO-ACT-02 : Propriétaire	EC-ACT-12 : Avis de confidentialité
EO-ACT-03 : Classification	EC-ACT-13 : Engagements de confidentialité ou de non-divulgence
EO-ACT-04 : Proportionnalité des mesures de protection	EO-ACT-14 : Demande de mise au rebut
EO-ACT-05 : Contrôle	EO-ACT-15 : Restitution du matériel
EC-ACT-06 : Supports amovibles	EO-ACT-16 : Stockage
EO-ACT-07 : Contrôles supplémentaires pour les supports amovibles	EO-ACT-17 : Validation
EO-ACT-08 : Messagerie	EO-ACT-18 : Notification
EO-ACT-09 : Echanges sécurisés avec les tiers	EC-ACT-19 : Vérification
EC-ACT-10 : Pièces jointes	EO-ACT-20 : Données à caractère personnel
	EO-ACT-21 : Perte et vol

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 4 sur 16
		Version	V2.0

2.1 Cartographie

EO-ACT-01	Inventaire
	Un inventaire des tous les actifs (logiciels, matériels, réseaux et informations manipulées) doit être réalisé et mis à jour.
Déclinaison Opérationnelle	Plusieurs inventaires matériels et logiciels existent : <ul style="list-style-type: none"> • Outil d'inventaire, type CMDB, pour l'ensemble des éléments de l'infrastructure ; • Outil d'inventaire pour les applications ; • Outil d'inventaire comptable.
	L'inventaire doit, à minima, lister les informations suivantes : <ul style="list-style-type: none"> • Le type d'actif (poste de travail, routeur, serveur, application web, etc.) ; • Les composants matériels (hardware) ; • La localisation (si possible) ; • Le nom du fabricant / propriétaire ; • Le nom et service du propriétaire ; • La version et numéro du système ou logiciel ; • L'adresse IP privée et/ou publique ; • La classification (<i>voir annexe 3.5</i>) ; • La date de livraison ; • La durée de garantie du matériel ; • La date de fin de maintenance pour les applications ; • Le numéro d'élément de l'équipement (ou de son lot) pour l'inventaire comptable.
	La liste des actifs doit être tenue à jour par les différentes équipes propriétaires de l'inventaire. Elle doit être revue à minima tous les ans.

EO-ACT-02	Propriétaire
	Un propriétaire doit être attribué à tout actif. Dans le cas d'une information où l'origine serait extérieure au CHU de Reims, l'entité réceptrice devient de facto, le propriétaire de l'actif.
Déclinaison Opérationnelle	Le propriétaire peut être une personne interne et active au CHU ou une unité fonctionnelle.
	En cas de départ de la personne, le propriétaire doit être remplacé. L'équipe propriétaire devient responsable de tout actif orphelin.
	A l'exception des actifs en stock (prêts à être déployer, en réparation, etc.) dans le périmètre des services informatiques, tout actif orphelin a, par défaut, une équipe comme propriétaire (ex : équipe poste de travail ou équipe réseau).

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 5 sur 16
		Version	V2.0


EO-ACT-03	Classification
	Les actifs, de type données, doivent être classés en fonction de leur sensibilité et évalués selon les besoins de sécurité en termes de Disponibilité, Intégrité et Confidentialité (DIC).
Déclinaison Opérationnelle	Le propriétaire de l'actif est responsable de la classification de sa sensibilité. Le RSSI valide cette classification.
	Dans les inventaires des actifs, la sensibilité de chaque actif est évaluée sur la base des critères DIC. <ul style="list-style-type: none"> - La disponibilité (D) : propriété d'un actif d'être accessible et utilisable à la demande d'une personne ou d'une entité autorisée dans les délais convenus. - L'intégrité (I) : propriété assurant qu'un actif n'a pas été modifié, altéré ou détruit de façon accidentelle ou non autorisée. - La confidentialité (C) : propriété selon laquelle un actif ne peut être divulgué ou rendu accessible à des individus, entités ou processus non autorisés.
	La grille de classification DIC est définie en Annexe.

2.2 Protection des données

EO-ACT-04	Proportionnalité des mesures de protection
	Les mesures de protection des données doivent être en adéquation avec leur sensibilité et doivent permettre de couvrir les risques sous-jacents.
Déclinaison Opérationnelle	Les collaborateurs du CHU de Reims doivent s'assurer de respecter les mesures de protection selon la sensibilisation des données concernées.
	Les mesures de sécurité à respecter selon le niveau de sensibilité des données sont définies en Annexe.

2.3 Protection des actifs

EO-ACT-05	Contrôle
	Le RSSI a autorité à contrôler l'inventaire des actifs ou demander des points de précision sur les mesures mises en place en relation avec les besoins de sécurité formulés.

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 6 sur 16
		Version	V2.0


Déclinaison Opérationnelle	Si le RSSI considère que les mesures mises en place sur l'actif ne respectent pas le principe de proportionnalité des mesures de protection pour l'actif considéré, le propriétaire doit les adapter en conséquence.
-----------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

EC-ACT-06	Supports amovibles
	L'usage des supports amovibles est par défaut interdit, sauf besoin explicite, validé par le RSSI.
Déclinaison Opérationnelle	L'usage des CD et DVD est interdit sauf dans le cadre des procédures dégradées qui pourraient nécessiter l'utilisation de DVD.
	L'usage des CD et DVD est exceptionnellement autorisé pour les médecins qui devraient visualiser des examens faits à l'extérieur.
	En cas d'accord d'utilisation d'une clé USB, un scan préalable est réalisé à l'aide de l'antivirus du poste où sera connectée la clé ou d'une Station de contrôle et de sécurisation de support amovible (en cours de déploiement)

EO-ACT-07	Contrôles supplémentaires sur les supports amovibles
	L'usage des clés USB doit être encadré.
Déclinaison Opérationnelle	Les utilisateurs ne sont autorisés qu'à brancher des clés USB dont ils connaissent la provenance. Ils sont également responsables de l'usage des clés qu'ils connectent à leurs postes de travail. L'usage des supports amovibles devra respecter les principes émis dans la Charte d'utilisation des supports externes.

2.4 Transfert de données

EO-ACT-08	Messagerie
	Les informations transitant par la messagerie électronique doivent être protégées de manière appropriée.
Déclinaison Opérationnelle	Des protocoles d'envoi de messages électroniques chiffrés doivent être mis en place et maintenus.
	Les serveurs de gestion de la messagerie doivent être maintenus à jour et protégés.
	Les utilisateurs doivent être sensibilisés de manière régulière aux bonnes pratiques de sécurité (notamment à respecter les mesures de

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 7 sur 16
		Version	V2.0

	sécurité en adéquation à la sensibilité des données) concernant l'utilisation de la messagerie électronique et aux procédures de protection de l'information.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------

EO-ACT-09	Echanges sécurisés avec les tiers
	Le CHU de Reims doit s'assurer de la sécurité de l'ensemble des échanges effectués entre son réseau et celui de ses partenaires.
Déclinaison Opérationnelle	Toute zone partenaire visant à échanger avec des services internes doit s'interconnecter via une technologie d'échange sécurisée.
	Tout tiers se connectant ou s'interconnectant au réseau du CHU de Reims doit utiliser des technologies sécurisées.
	Une clause relative à la sécurisation et la bonne utilisation du réseau doit être inscrite dans la relation contractuelle avec chaque partenaire. Se référer à la Politique de gestion des fournisseurs pour la mise en place du contrat.

EC-ACT-10	Pièces jointes
	L'utilisation d'une messagerie électronique pour communiquer des documents sous forme de pièces-jointes est fortement déconseillée pour des raisons de sécurité.
Déclinaison Opérationnelle	<p>Les pièces-jointes représentent des sources de risques du point de vue de la sécurité de l'information. Il est ainsi fortement recommandé de privilégier l'envoi de documents sous la forme de liens permettant de rejoindre un espace de dépôt sécurisé (par exemple une GED). Les accès aux espaces sécurisés doivent être restreints pour respecter les besoins de la sécurité.</p> <p>S'il était avéré que des pièces-jointes sensibles ne pouvaient être mise à disposition par un autre moyen, alors celles-ci devront être chiffrées, comme il est inscrit dans la Politique de Sécurité du Système d'Information.</p>

EO-ACT-11	Besoin d'en connaître
	Ce principe doit limiter les accès illégitimes des données par des personnes n'ayant pas l'autorisation d'en prendre connaissance.
Déclinaison Opérationnelle	Le propriétaire de l'information, ainsi que sa hiérarchie sont responsables de l'accès de l'information aux différents destinataires.

EC-ACT-12	Avis de confidentialité
------------------	--------------------------------

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 8 sur 16
		Version	V2.0

	Une information reçue par erreur par un destinataire doit être supprimée par celui-ci. L'émetteur du message doit également être avisé.
Déclinaison Opérationnelle	Toute personne qui reçoit par erreur une information doit prévenir l'expéditeur de celle-ci par email et détruire l'information, selon les moyens appropriés.


	Engagements de confidentialité ou de non-divulgaration
EC-ACT-13	Le CHU de Reims doit identifier, documenter et revoir régulièrement les exigences en matière d'engagements de confidentialité et de non-divulgaration conformément à ses besoins en matière de protection de l'information.
Déclinaison Opérationnelle	Un processus de veille sur les exigences en matière d'engagements de confidentialité et de non-divulgaration doit être formalisé et revu régulièrement.

2.5 Mise au rebut

	Demande de mise au rebut
EO-ACT-14	La mise au rebut doit suivre une procédure stricte intervenant en cas d'obsolescence ou de dysfonctionnement.
Déclinaison Opérationnelle	Une liste des actifs à mettre au rebut doit être maintenue à jour et archivée par l'équipe propriétaire de l'actif.

	Restitution du matériel
EO-ACT-15	La restitution du matériel doit suivre une procédure stricte intervenant en cas de sortie d'un collaborateur.
Déclinaison Opérationnelle	Tous les collaborateurs doivent restituer la totalité des actifs du CHU qu'ils ont en leur possession, si ces actifs leurs sont nominativement affectés, au terme de la période d'emploi ou du contrat.
	Les actifs doivent être restitués à la DSN en suivant la procédure de restitution d'un matériel.

EO-ACT-16	Stockage
------------------	-----------------

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 9 sur 16
		Version	V2.0

	Le matériel à mettre au rebut doit être stocké dans un lieu protégé par contrôle d'accès et limité à un personnel restreint.
Déclinaison Opérationnelle	Une liste des entrées et des sorties de matériel (description, date, personne procédant au transport) doit être maintenue à jour et archivée par l'équipe propriétaire de l'actif.
	Les postes de travail sont stockés sous clés dans le local de stockage prévu à cet effet. Le prestataire vient ensuite les récupérer pour la mise au rebut.
	Les équipements d'infrastructure sont conservés dans le datacenter et protégés par un accès à badge. Le prestataire vient ensuite les récupérer pour la mise au rebut.

EO-ACT-17	Validation
	Après traitement, un PV correspondant à l'action réalisée (destruction ou recyclage) doit être créé.
Déclinaison Opérationnelle	Le PV attestant de la destruction effective ou du recyclage de l'actif doit être archivé par la Direction du patrimoine.
	Un contrat DEEE devra être passé entre le prestataire en charge de la mise au rebut et le CHU de Reims.

2.6 Transfert physique des supports

EO-ACT-18	Notification
	Le mouvement doit obligatoirement faire l'objet d'une traçabilité précise dans la mise à jour des inventaires.
Déclinaison Opérationnelle	Les seuls transferts effectués au sein du CHU de Reims sont ceux d'actifs entre les différents sites du CHU de Reims ou en interne à un site du CHU de Reims.

EC-ACT-19	Vérification
	L'état physique de l'actif devra être vérifié lors de son arrivée afin de s'assurer que l'acheminement n'a pas causé de dommage.
Déclinaison Opérationnelle	Un bon de réception peut venir alimenter l'inventaire des actifs.


	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 10 sur 16
		Version	V2.0

2.7 Réglementaire

EO-ACT-20	Données à caractère personnel
	Les données à caractère personnel doivent faire l'objet de mesures de sécurité proportionnelles à leur sensibilité et être supprimées selon les durées de conservation préalablement définies.
Déclinaison Opérationnelle	La manipulation de données à caractère personnel doit respecter les règles définies dans la Politique de Sécurité du Système d'Information et la charte utilisateur.
	Toute donnée à caractère personnel doit être classifiée comme « Confidentiel » au sens de la classification des actifs du CHU de Reims.
	Tout export de masse de données à caractère personnel en dehors du SI du CHU de Reims doit faire l'objet d'une validation préalable du RSSI et du DPD.
	Les durées de conservation sont définies par le responsable de traitement selon le cadre légal ou la finalité. Le DPD est garant de la définition de ces durées.

2.8 Vol et perte de matériel

EO-ACT-21	Perte et Vol
	En cas de perte ou de vol de matériel, le collaborateur du CHU de Reims doit prévenir le support dans les plus brefs délais.
Déclinaison Opérationnelle	Les interlocuteurs à contacter sont le centre de support. Le support pourra alors fournir les informations nécessaires à la plainte : (numéro machine, description de l'actif...) Le support devra prendre les mesures possibles pour bloquer la machine à distance ou géolocaliser la machine.
	Le support devra prévenir le DPD qui décidera si une déclaration à la CNIL est nécessaire (présence ou non de données sensibles sur le matériel volé).
	En cas de vol de matériel au sein du CHU, la cellule Sûreté, Vigilance et Protection a la charge de porter plainte.
	En cas de vol de matériel en dehors du CHU, l'agent a la charge de porter plainte.

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 11 sur 16
		Version	V2.0

3 Annexe

3.1 Glossaire

Acronyme	Définition
CMDB	Configuration Management Database (Base de données de gestion de configuration)
DEEE	Déchets d'équipements électriques et électroniques
DIC	Besoins de sécurité des systèmes d'information (Disponibilité, Intégrité, Confidentialité)
DPD	Délégué à la Protection des Données
RSSI	Responsable de la Sécurité du Système d'Information
SI	Système d'Information

3.2 Références

Références	Description
Chapitre de la norme ISO 27001 Annexe A	ISO 27001 A.8.1.1 Inventaire des actifs A.8.1.2 Propriété des actifs A.8.1.3 Utilisation correcte des actifs A.8.1.4 Restitution des actifs A.8.2.1 Classification des informations A.8.2.3 Manipulation des actifs A.8.3.2 Mise au rebut des supports A.8.3.3 Transfert physique des supports A.13.2.1 Politiques et procédures de transfert de l'information A.13.2.2 Accords en matière de transfert de l'information A.13.2.3 Messagerie électronique A.13.2.4 Engagements de confidentialité ou de non-divulgaration A.18.1.4 Protection de la vie privée et protection des données à caractère personnel
Documents de référence	Ce document fait notamment référence à : <ul style="list-style-type: none"> • La PSSI ; • La Politique de gestion des fournisseurs ; • La Charte Utilisateur ; • La Charte d'utilisation des supports externes.


3.3 RACI

Exigence	RSSI	DPD	Equipe propriétaire de l'actif	Support	Propriétaire	Utilisateur
EO – ACT – 01	A				R	I
EO – ACT – 02		I			R	
EO – ACT – 03	A				R	I
EC – ACT – 04	A				R	I
EO – ACT – 05	R				C	
EC – ACT – 06	A					I
EO – ACT – 07	C					R
EO – ACT – 08	A/C		R			
EO – ACT – 09	A/C				R	
EC – ACT – 10	A				I	R
EO – ACT – 11	A				R	I
EC – ACT – 12	A				R	I
EC – ACT – 13	R	C				I
EO – ACT – 14	A		R		C	I
EO – ACT – 15	A		R		I	
EO – ACT – 16	A		R		C	
EO – ACT – 17	A		R		I	
EO – ACT – 18	A		R			
EC – ACT – 19	A		R		I	
EO – ACT – 20	A	A			R	I
EO – ACT – 21	I	I		I		R

R : Responsable, **A** : Approbateur, **C** : Consulté, **I** : Informé


3.4 Revue de la politique

Cette politique doit être revue annuellement.

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 13 sur 16
		Version	V2.0

3.5 Grille de classification DICT

Niveaux	Confidentialité	Intégrité	Disponibilité
1	PUBLIQUE : La divulgation de l'information n'a aucun impact en termes d'image ou de compétitivité pour l'entreprise	AUCUNE : Une modification de l'information n'a pas d'impact pour l'entreprise	FAIBLE : L'arrêt prolongé de l'application ou la perte des données n'a pas d'impact pour l'entreprise
2	INTERNE : La divulgation de l'information, utilisée par des employés pour mener à bien leur mission et n'ayant pas vocation à être diffusée, peut perturber le fonctionnement de l'entreprise	STANDARD : Une modification de l'information peut perturber le fonctionnement de l'entreprise, et doit être détectée	MOYENNE : L'arrêt prolongé de l'application ou la perte des données perturbe le fonctionnement de l'entreprise, sans impact vis-à-vis de l'externe
3	CONFIDENTIELLE : La divulgation de l'information peut porter atteinte à la vie privée des employés ou adhérents et dégrader fortement le fonctionnement de l'entreprise	RENFORCÉE : Une modification de l'information peut dégrader le fonctionnement de l'entreprise ou être visible des adhérents, et doit être détectée puis corrigée automatiquement	FORTE : L'arrêt de l'application ou la perte des données dégrade fortement le fonctionnement de l'entreprise, et est visible par les adhérents
4	TRES CONFIDENTIELLE : La divulgation de l'information peut impliquer une perte de compétitivité totale de l'entreprise	INALTÉRABLE : Une modification des données peut entraîner un dysfonctionnement important et mettre en péril l'entreprise, et ne doit pas être possible	AUCUNE INDISPONIBILITÉ, NI PERTE DE DONNÉES TOLERÉE : Tout arrêt ou perte de données met en péril l'entreprise

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 14 sur 16
		Version	V2.0

3.6 Mesures de sécurité

	1	2	3	4
Confidentialité	Création - Mention du niveau de confidentialité sur les documents Impression - Impression limitée au strict nécessaire	Création - Niveau 1 + mention du propriétaire de l'information sur les documents Impression - Utilisation de la fonction d'impression sécurisée ou d'une imprimante dédiée, retrait du document dans les meilleurs délais par le propriétaire ou le dépositaire de l'information Diffusion/Transmission - Diffusion dans la limite du besoin d'en connaître - Diffusion interdite vers une messagerie personnelle - Diffusion auprès d'un partenaire de confiance uniquement après autorisation du propriétaire des données et accord de confidentialité Stockage - Chiffrement des données sur support amovible	Création - Niveau 2 + mention des personnes pouvant accéder à l'information de manière générique ou nominative - Mention de la date de création et du délai recommandé de conservation du niveau de classification Impression - Marquage et identification du dépositaire de l'exemplaire dupliqué Diffusion/Transmission - Diffusion restreinte à une liste finie de personne, un service ou un département - Diffusion auprès d'un partenaire de confiance e données personnelles uniquement après validation SSI - Envoi des impressions sous double enveloppes fermées - Chiffrement obligatoire de l'information ou du flux en transport Stockage	Création - Indication des personnes pouvant accéder à l'information de manière nominative uniquement Diffusion/Transmission - Diffusion vers une liste de personne finie uniquement - Chiffrement obligatoire de l'information ou du flux en transport Stockage - Chiffrement unitaire de la donnée - Stockage sur support amovible interdit - Stockage des impressions dans des armoires fortes Destruction - Utilisation d'une broyeuse pour la mise au rebut des impressions - Destruction physique des disques durs

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 15 sur 16
		Version	V2.0

		<ul style="list-style-type: none"> - Stockage des supports amovibles et des impressions dans des zones protégées sous clés Destruction <ul style="list-style-type: none"> - Utilisation de dispositifs d'effacement classique 	<ul style="list-style-type: none"> - Chiffrement des données sur support fixe Destruction <ul style="list-style-type: none"> - Utilisation de dispositifs rendant impossible toute tentative de récupération ou reconstitution de l'information après destruction (ex : logiciels d'effacement de disque dur certifiés) - Mise au rebut des impressions papiers dans un container sécurisé interdisant la récupération et destruction sécurisée - Utilisation recommandée d'une broyeuse 	
Intégrité	Diffusion/Transmission <ul style="list-style-type: none"> - Utilisation préconisée des mécanismes déjà présents nativement dans les solutions / protocoles / produits mis en œuvre - Pas d'autre mécanisme de détection et correction des erreurs en transport supplémentaire requis Stockage <ul style="list-style-type: none"> - Utilisation préconisée des mécanismes déjà présents nativement dans les solutions / protocoles / produits mis en œuvre - Pas d'autre mécanisme de détection et correction des erreurs en stockage supplémentaire requis 	Diffusion/Transmission <ul style="list-style-type: none"> - Mise en œuvre de mécanismes dédiés à la détection des erreurs en transport par redondance complète de l'information et comparaison ou comparaison d'informations calculées à partir de l'information d'origine ou transport par des canaux différents - Mise en œuvre de procédures de correction manuelle en cas de détection d'erreur Stockage <ul style="list-style-type: none"> - Mise en œuvre de mécanismes dédiés à la détection des erreurs en stockage par redondance complète de l'information et comparaison ou comparaison d'informations 	Diffusion/Transmission <ul style="list-style-type: none"> - Mise en œuvre de mécanismes dédiés à la correction des erreurs en transport par retransmission ou autocorrection Stockage <ul style="list-style-type: none"> - Mise en œuvre de mécanismes dédiés à l'autocorrection des erreurs en stockage 	Diffusion/Transmission <ul style="list-style-type: none"> - Se reporter au niveau 3 Stockage <ul style="list-style-type: none"> - Utilisation d'un medium de stockage présentant des caractéristiques permettant de garantir l'intégrité

	Groupement Hospitalier Universitaire de Champagne		
	Politique de gestion des actifs et transfert de données	Date de création	30/09/2024
		Page	Page 16 sur 16
		Version	V2.0

		calculées à partir de l'information d'origine - Mise en œuvre de procédures de correction manuelle en cas de détection d'erreur. Se reporter aux mécanismes de remise en disponibilité de niveau 2		
Disponibilité	Sauvegarde des données/traitements - Pas de mécanisme technique de sauvegarde requis Mécanisme de remise en disponibilité après perte de disponibilité - Pas de mécanisme technique de remise en disponibilité requis Moyens organisationnels et humains - Support classique durant les jours et heures ouvrés de bureau Sites - Pas d'exigence	Sauvegarde des données/traitements - Sauvegarde programmée des données/traitements à fréquence fixe Mécanisme de remise en disponibilité après perte de disponibilité - Reconstruction manuelle de l'environnement à partir des sauvegardes Moyens organisationnels et humains - Réactivité en horaires étendus Sites - Machines distinctes, même site géographique	Sauvegarde des données/traitements - Réplication asynchrone et points de synchronisation sur un environnement tiers passif Mécanisme de remise en disponibilité après perte de disponibilité - Bascule manuelle ou automatique sur un environnement tiers passif de secours sur lequel les données/traitements ont été répliqués Moyens organisationnels et humains - Réactivité en horaires étendus et mise en place d'astreintes Sites - Machines distinctes sur 2 sites distincts géographiquement	Sauvegarde des données/traitements - Réplication synchrone des données et/ou traitement sur un environnement tiers actif Mécanisme de remise en disponibilité après perte de disponibilité - Bascule automatique sur un environnement de secours actif sur lequel les données/traitements ont été répliqués Moyens organisationnels et humains - Réactivité permanente : 7 x 24 x 52 Sites - Se reporter au niveau 3