

	Politique GHUC		
	Groupe Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 1 sur 10
		Version :	1

	Rédaction	Forme vérifiée par DQGDR	Validation
Nom	PETIT Virginie	PETIT Virginie (22/02/2024)	BIAIS Hilde (22/02/2024)

Sommaire	
Rédaction.....	1
Introduction.....	2
Contexte	2
Objectifs	2
Périmètre d’application.....	2
Exigences	3
Annexe	9
Glossaire	9
Références.....	9
RACI	10
Revue de la politique	10

	Politique GHUC		
	Groupeement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 2 sur 10
		Version :	1

Introduction

Contexte

La gestion de la sécurité dans la relation avec les fournisseurs est un enjeu majeur permettant le maintien du niveau de sécurité défini par le CHU de Reims.

Les fournisseurs sont toutes les entreprises ou entités qui fournissent des biens ou des services et qui sont susceptibles d'accéder à des informations numériques du CHU de Reims, de les traiter, de les stocker, de les communiquer ou de fournir des composants à l'infrastructure informatique du CHU de Reims.

Objectifs

Les objectifs de cette politique sont :

- Décrire les rôles et responsabilités entre les acteurs du CHU de Reims et ses fournisseurs (qu'ils soient titulaires du marché, ou répondant à un appel d'offre.
- Définir les exigences de sécurité que l'organisation fixe à ses fournisseurs pour atteindre les objectifs de sécurité.

Périmètre d'application

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

- La Direction Générale ;
- Le RSSI ;
- Le service achat et juridique ;
- Les responsables métiers ;
- Les tiers (fournisseurs, prestataires, sous-traitants, ...).

	Politique GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 3 sur 10
		Version :	1

Exigences

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

Les Exigences sont Obligatoires : **EO**, ou Conseillées : **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-FOU-01** : Sélection d'un fournisseur
- **EO-FOU-02** : Accès et habilitations des fournisseurs
- **EO-FOU-03** : Mises à jour des équipements ou serveurs gérés par les fournisseurs
- **EO-FOU-04** : Sécurité des données hébergées par les fournisseurs
- **EO-FOU-05** : Traces et journaux d'activité des fournisseurs
- **EO-FOU-06** : Contrat et clauses contractuelles
- **EO-FOU-07** : Audit des fournisseurs
- **EO-FOU-08** : Suivi des prestations
- **EC-FOU-09** : Comité et outil de suivi des fournisseurs
- **EO-FOU-10** : Sous-traitance ultérieure
- **EO-FOU-11** : Gestion des contrats

	Politique GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 4 sur 10
		Version :	1

EO-FOU-01	Sélection d'un fournisseur
	Les fournisseurs doivent être sélectionnés en fonction de critères de sécurité définis par le CHU de Reims dans la PSSI.
Déclinaison Opérationnelle	En cas de nouveau besoin faisant appel à un fournisseur, le service Achat sollicite l'équipe sécurité en phase d'étude afin d'intégrer la sécurité au processus de sélection du fournisseur.
	Un chef de projet est identifié au sein du CHU et il sollicite l'équipe sécurité pour identifier les besoins de sécurité associés à la prestation afin de sélectionner les exigences à intégrer dans le contrat.
	Si la prestation inclut l'hébergement de données de santé, le tiers doit alors disposer de la certification hébergeur de données de santé sur le périmètre concerné par la prestation.
	Le cahier des charges intègre les exigences de sécurité en accord avec les critères de sécurité définis.
	Dans le cas d'une réponse à appel d'offre, le fournisseur devra indiquer les mesures de sécurité qu'il entend mettre en place afin de répondre aux exigences.

EO-FOU-02	Accès et habilitations des fournisseurs
	Les accès des fournisseurs à l'information, aux applications et aux systèmes du CHU de Reims doivent être encadrés par des habilitations.
Déclinaison Opérationnelle	Le tiers s'engage à appliquer les mesures de contrôle d'accès et à utiliser les outils sur les équipements et les serveurs fournissant un service au CHU de Reims sur lesquels chaque collaborateur du tiers étant appelé à y accéder devra disposer d'un compte nominatif, sauf exception.
	Les mots de passe sur les équipements, serveurs ou applications sous la responsabilité du tiers et fournissant un service au CHU de Reims doivent respecter des règles de complexité et de fréquence de renouvellement définies dans la charte de droit d'accès distants.
	Les règles de gestion des accès et des habilitations sur les équipements ou serveurs sous la responsabilité du tiers et fournissant un service au CHU de Reims devront être conformes à celles énoncées dans la politique de gestion des accès et des habilitations du CHU de Reims.
	Le chef de projet devra mettre en place une revue annuelle des accès et habilitations du tiers.

	Politique GHUC		
	Groupeement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 5 sur 10
		Version :	1

	Les accès à distance devront être contrôlés par le bastion en place au CHU de Reims
--	---

EO-FOU-03	Mises à jour des équipements ou serveurs gérés par les fournisseurs
	Les équipements ou serveurs gérés par les fournisseurs doivent être mis à jour.
Déclinaison Opérationnelle	Le tiers applique les mises à jour et correctifs de sécurité sur les équipements ou serveurs fournissant un service au CHU de Reims dont il a la responsabilité en conformité avec la politique de maintien en condition des applications du CHU de Reims.
	Le tiers n'emploie pas de versions de systèmes ou d'applications obsolètes ou non supportées par leur éditeur pour fournir un service au CHU de Reims.

EO-FOU-04	Sécurité des données hébergées par les fournisseurs
	Les fournisseurs doivent assurer la sécurité des données qu'ils hébergent pour le compte du CHU de Reims.
Déclinaison Opérationnelle	Les données sensibles du CHU de Reims dont la responsabilité est déléguée au tiers doivent faire l'objet de mesures de contrôle d'intégrité. Le tiers doit être certifié « Hébergeur de Données de Santé » et les données doivent être stockées en Europe, de préférence. Il pourra être demandé au tiers sa certification HDS.
	Lors de la mise au rebut de ses supports de stockage endommagés ou obsolètes, des mesures de destruction sécurisée des données du CHU doivent être prises.
	La politique de sauvegarde doit être définie.

EO-FOU-05	Traces et journaux d'activité des fournisseurs
	Les traces et journaux d'activité générés par les équipements et serveurs opérés par des fournisseurs doivent être conservés.
Déclinaison Opérationnelle	Les journaux d'activité des équipements ou serveurs opérés par le tiers et fournissant un service au CHU de Reims doivent être archivés et leur intégrité doit être protégée.

	Politique GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 6 sur 10
		Version :	1

	La journalisation mise en place par le tiers doit pouvoir faire un lien entre une action et l'identifiant de l'utilisateur responsable de cette action. Ces traces doivent être conservées (36 semaines), mises à disposition du CHU, à sa demande et intégrées dans l'agrégateur de traces du CHU.
EO-FOU-06	Contrat et clauses contractuelles
	Les contrats doivent contenir des clauses de sécurité applicables au périmètre et contexte de la prestation.
Déclinaison Opérationnelle	Tout contrat doit inclure les éléments suivants : <ul style="list-style-type: none"> • Les exigences de sécurité à mettre en place par le prestataire au regard du périmètre de la prestation (PAS). Le PAS devrait s'appuyer sur les chapitres de l'ISO27002 ; • Les exigences relatives à la protection des données à caractère personnel au regard des données manipulées dans le cadre de la prestation ; • Une clause d'audit et de contrôle qui assure le droit au CHU de Reims d'auditer les fournisseurs afin de vérifier que les exigences de sécurité présentes dans le contrat sont bien implémentées ; • Les obligations et disponibilités de service ; • Une clause de réversibilité et de remédiation est à ajouter en fonction de la prestation, pour permettre de garantir la continuité d'activité en cas d'arrêt du service et/ou de fin de marché.
	L'accord cadre sur la protection des données doit être signé par les fournisseurs.
	Le PCA et le PRA des fournisseurs de prestation SaaS doivent être fournis au CHU de Reims.

EO-FOU-07	Audit des fournisseurs
	Les fournisseurs identifiés comme « sensibles » doivent être régulièrement audités par le CHU de Reims.
Déclinaison Opérationnelle	Un programme d'audit des fournisseurs doit être défini annuellement. Ce programme doit inclure un nombre défini de fournisseurs à auditer. Ces audits ont pour objectif de vérifier le respect des mesures de sécurité convenues avec le fournisseur et intégrées au contrat.
	En annexe, la liste des fournisseurs à auditer et les critères de sensibilité.

	Politique GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 7 sur 10
		Version :	1

	Ils peuvent être réalisés de manière : <ul style="list-style-type: none"> • Déclarative au travers d'un questionnaire ; • Au travers d'entretien et d'analyse sur site en cas de points spécifiques à vérifier.
	Ces audits font l'objet d'un rapport transmis aux fournisseurs, comprenant une appréciation (ex : Favorable, Sous surveillance, Défavorable).
	A la suite du rapport, un plan d'action est défini conjointement et mis en œuvre par le fournisseur.

EO-FOU-08	Suivi des prestations
	Un suivi des fournisseurs doit être défini et mis en œuvre.
Déclinaison Opérationnelle	Une validation de service fait doit être produite par le bénéficiaire.
	À la fin de la collaboration, le responsable du contrat valide la bonne clôture de celui-ci. En particulier, il s'assure de la suspension de l'ensemble des accès et habilitations mis à disposition des tiers.
	En cas d'expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le tiers s'engage : <ul style="list-style-type: none"> - à éviter toute interruption ou baisse de qualité des services avant la fin du contrat ; - à assurer les opérations qui permettront au CHU de Reims d'avoir toute la maîtrise nécessaire afin de reprendre ou de faire reprendre par un tiers les services dans les meilleures conditions (transfert de compétences, documents explicatifs, etc.).

EC-FOU-09	Comité et outil de suivi des fournisseurs
	Un suivi spécifique des fournisseurs identifiés comme « sensibles », en fonction de la nature de la prestation, peut être défini et mis en œuvre.
Déclinaison Opérationnelle	En fonction de la nature de la prestation, un comité de suivi des fournisseurs peut être mis en place. Il permet de suivre la performance de la prestation, la relation client/ fournisseur, le respect des exigences de sécurité et SLA éventuels. Ce suivi est à la charge du chef de projet et peut demander une intervention de l'équipe sécurité si besoin sur certains aspects.
	L'outil ADELE doit être utilisé pour déclarer les litiges avec les fournisseurs via une demande à la Sécurité « Demande d'expertise Sécurité et RGPD ». La performance du fournisseur peut également être suivie sur cet outil.

	Politique GHUC		
	Groupeement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 8 sur 10
		Version :	1

	Des indicateurs peuvent être mis en place afin de suivre la performance des titulaires sur le marché. Ces indications émaneront des prérequis Fournisseurs.
--	---

EO-FOU-10	Sous-traitance ultérieure
	Le sous-traitant ultérieur (sous-traitant du fournisseur) doit hériter des mesures de sécurité définies dans le cadre du contrat.
Déclinaison Opérationnelle	La sous-traitance des prestataires doit être déclarée au CHU de Reims.
	En cas de sous-traitance ultérieure, le prestataire doit veiller à ce que son sous-traitant applique à son tour les mesures de sécurité définies dans le contrat avec le CHU de Reims afin d'éviter une dégradation du niveau de sécurité global de la prestation.
	Un audit de sous-traitant peut être demandé par le RSSI du CHU de Reims.
	Le mandataire du marché est responsable de ses sous-traitants.

EO-FOU-11	Gestion des contrats
	Les contrats conclus avec les fournisseurs sont des données sensibles et doivent être gérés de manière sécurisée.
Déclinaison Opérationnelle	Les exigences de sécurité à appliquer sont définies dans la politique de gestion des actifs et transfert de données.

	Politique GHUC		
	Groupeement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 9 sur 10
		Version :	1

Annexe

Glossaire

Acronyme	Définition
PAS	Plan d'Assurance Sécurité
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
PSSI	Politique de Sécurité des Systèmes d'Information
RGPD	Règlement Général sur la Protection des Données à caractère personnel
RSSI	Responsable Sécurité des Systèmes d'Information
SaaS	Software as a Service
SLA	Service Level Agreement (Accord de niveau de service)
Sous-traitance	Contrat par lequel une entreprise demande à une autre entreprise de réaliser une partie de sa production

Références

Références	Description
Chapitre de la norme ISO 27001 Annexe A	<u>ISO 27001</u> A.15.1.1 Politique de sécurité dans les relations avec les fournisseurs A.15.1.2 La sécurité dans les accords conclus avec les fournisseurs A.15.1.3 Chaîne d'approvisionnement informatique A.15.2.1 Surveillance et revue des services des fournisseurs A.15.2.2 Gestion des changements apportés dans les services des fournisseurs
Documents de référence	Ce document fait notamment référence à : <ul style="list-style-type: none"> • La PSSI ; • Charte de droit d'accès distants ; • La politique de maintien en condition des applications ; • Politique de sauvegarde ; • Politique de gestion des actifs et transfert de données ;

	Politique GHUC		
	Groupement Hospitalier Universitaire de Champagne		
	POLITIQUE DE GESTION DES FOURNISSEURS	Référence :	SI-POLG-007
		Date de création :	27/07/2022
		Page :	Page 10 sur 10
		Version :	1

	<ul style="list-style-type: none"> • Accord-cadre sur la protection des données. • Prérequis Fournisseurs ((RS_PR_Fournisseur_V0.1) • Liste des fournisseurs à auditer
--	---

RACI

Exigence	RSSI/DPD	Direction des Services Numériques	Service achat, juridique, Ressources Humaines	Direction générale	Chef de projet
EO – FOU – 01	C	A	C	I	R
EO – FOU – 02	C	I			R/A
EO – FOU – 03	C	I			R/A
EO – FOU – 04	R	I			A
EO – FOU – 05	C	R/A			I
EO – FOU – 06	C	A	C	A	R
EO – FOU – 07	R	A	C	I	C
EO – FOU – 08	I	I			R/A
EC – FOU – 09	C	C			R/A
EO – FOU – 10	C	I	C		R/A
EO – FOU – 11	C	A	C		R

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

Revue de la politique

Le politique de gestion des fournisseurs doit être revue annuellement.