

Fiche de poste « Technicien Système - infra - réseau »			
	Sites : Albertville, Moutiers et St Pierre d'Albigny (Dubettier)	Version n° 1.0	MODE OPERATOIRE
		Diffusé en : Sept 2026	CODE
			Page 1 sur 7

1° Objet et Mots-clés

Ce document présente la fiche de poste d'un « Technicien Système - infra - réseau » du CHAM.

Mots-clés : fiche de poste, Technicien Système - infra - réseau

2° Domaine d'application

Personnels de la DSIO, RH

3° Définitions ou abréviations

DSIO : Direction des Systèmes d'Information et de l'Organisation

SI : Système d'Information

4° Documents associés / Annexes

Aucun

5° Références bibliographiques

Aucun

6° Historique des mises à jour et tableau des visas

N° version	Date	Historique des mises à jour (indications des modifications)	N° des pages modifiées
Travail	01/09/2026	Création	Toutes
1.0	08/09/2021	Validation de la version	Toutes

Rédaction initiale	DSIO : JM. Rasle (Directeur des Systèmes d'Information et de l'Organisation)	08/09/2026
Relecture	Services RH	08/09/2026
Validation	DSIO : JM. RASLE (Directeur des Systèmes d'Information et de l'Organisation)	08/09/2026

7° Description de l'activité

1- LIEU D'AFFECTATION AGENT

Service informatique du CHAM
Informatique de l'hôpital Dubettier à St Pierre D'Albigny

2- RESPONSABLE(S) HIERARCHIQUE(S) / FONCTIONNEL(S)

Rattachement hiérarchique : travaille sous l'autorité du Directeur des Systèmes d'Information et de l'Organisation du CHAM
Possibles actions pour l'hôpital Dubettier à St Pierre D'Albigny, sans rattachement hiérarchique ou fonctionnel au Directeur de cet hôpital.

3- MISSIONS

Il assure la gestion courante de l'exploitation système dans le respect des plannings et de la qualité attendue. Il surveille l'activité des équipements informatiques physiques et logiques associés, afin de garantir le bon fonctionnement de l'ensemble des systèmes hébergeant les applications, dans le cadre des normes, méthodes d'exploitation et de sécurité.

Il contribue à la résolution des incidents systèmes de niveau 1 et résout les incidents systèmes de niveau 2.

Il met en production, administre et exploite des solutions de sécurité (antivirus, supervision, bastion, IAM, etc.). Il participe au bon fonctionnement des solutions de sécurité en garantissant le maintien en conditions opérationnelles et de sécurité.

Il réalise des évaluations techniques de la sécurité des environnements informatiques. Il identifie et/ou analyse les vulnérabilités et propose des actions de remédiation. Il peut réaliser différents types d'audits en fonction de son périmètre d'activité (AD, droits applicatifs, habilitations, etc.). Il s'assure de la conformité aux politiques internes et aux réglementations qui s'appliquent à l'établissement. Il contrôle que les politiques et règles de sécurité définies pour assurer le maintien en conditions de sécurité sont mises en œuvre, respectées et efficaces.

Il est capable d'être force de proposition sur le domaine système-infra-réseau.

4- INTERACTIONS PROFESSIONNELLES

- Avec les utilisateurs et référents métiers
- Avec les prestataires et fournisseurs
- Avec le RSSI et le DPO du CHAM ou du GHT afin de s'assurer du respect des règles de sécurité préconisées
- Qualités : discrétion, secret professionnel, rigueur

5- DESCRIPTION DES ACTIVITES ET TACHES

ADMINISTRATION :

- Administrer et maintenir les serveurs physiques et virtuels, notamment les environnements Windows Server et, selon les besoins, Linux.
- Participer à l'exploitation des infrastructures de virtualisation, de stockage et de sauvegarde.
- Possède une vision globale et actualisée du SI.
- Gérer les services d'infrastructure : annuaire Active Directory, DNS, DHCP, services de fichiers, impressions, messagerie ou services associés.
- Suit et analyse les performances, met en place des mesures susceptibles d'améliorer la qualité ou la productivité de l'outil.
- Installer, configurer et maintenir les systèmes d'exploitation, logiciels techniques et outils d'administration.
- Réaliser les mises à jour de sécurité, suivre les correctifs et contribuer au traitement des vulnérabilités.
- Participer à la supervision des réseaux, à l'analyse des incidents et à l'optimisation des performances.

INSTALLATION ET TESTS :

- S'assure de la disponibilité correcte quotidienne des réseaux
- Supervise et gère l'infrastructure des réseaux locaux et distants (LAN / WAN / VPN) : installe, teste, supervise la partie active de la connectique et passive du matériel informatique (postes et serveurs connectés) et logiciels réseau
- Respecte les procédures d'installation, de connexion... des matériels et des logiciels
- Installe les mises à jour
- Effectue les tests des équipements réseaux

EXPLOITATION :

- Installe et intègre des nouveaux outils systèmes (évolutions, migrations, nouveau projets) dans l'environnement de production.
- Gère les droits d'accès aux serveurs et aux applications dont il a la charge en fonction des profils.
- Contribue à la résolution des incidents systèmes de niveau 1.
- Traite les incidents ou anomalies systèmes de niveau 2 et 3 à partir des demandes internes : diagnostic de l'incident, identification, formulation et suivi de sa résolution. Trace les éléments sur l'outil Octopus.
- Assure en priorité la maintenance des systèmes orientés Windows/Linux et l'hyperviseur VmWare

SUPPORT :

- Prendre en charge les incidents et demandes relevant du périmètre systèmes, réseaux et infrastructures.
- Assurer un diagnostic technique, mettre en œuvre les actions correctives et informer les utilisateurs ou équipes concernées.
- Propose des améliorations pour optimiser les ressources existantes et leur organisation
- Participer aux actions de support aux équipes informatiques et aux projets de déploiement applicatif ou matériel.

MAINTENANCE ET SÉCURITÉ :

- Gère les accès aux ressources du SI (en général).
- Gère les évolutions et la maintenance des matériels, des logiciels et du système.

ÉTUDES :

- Effectue des études de préconisation et d'implantation des matériels, outils et logiciels adaptés.
- Effectue une veille technologique sur les différents aspects de l'infrastructure système et de communication (matériels, logiciels, architecture, protocole, mode de transferts).

QUALITÉ, SÉCURITÉ :

- Alerte sa hiérarchie sur tout incident qui est « hors norme » et alerte les autres départements de la DSIO en cas de suspicion d'escalade.
- Applique les plans de secours (PCA/PRA).
- Rédige et applique les documentations techniques et d'exploitation des systèmes relatives à son secteur d'activité.
- Participe au respect des procédures et d'assurance de qualité et de sécurité du SI.

SUIVI :

- Est force de proposition pour l'évolution des systèmes en anticipant les besoins en termes de dimensionnement et de sécurité des systèmes.

RELATIONS FOURNISSEURS :

- Est en relation avec les fournisseurs pour assurer les dépannages/évolutions/migration et suivre leurs interventions

6- COMPETENCES REQUISES

COMPETENCES TECHNIQUES

- Bonne maîtrise des environnements Windows poste de travail et Windows Server.
- Connaissances des services d'annuaire, notamment Active Directory, DNS, DHCP et stratégies de groupe.
- Connaissances en virtualisation, stockage, sauvegarde et restauration.
- Maîtrise des fondamentaux réseau : TCP/IP, VLAN, routage, commutation, Wi-Fi, pare-feu et filtrage.
- Connaissance des outils de supervision, de gestion de parc, de ticketing et de documentation.
- Connaissances en cybersécurité : gestion des accès, mises à jour, journalisation, segmentation réseau, sauvegarde et protection contre les rançongiciels.
- Capacité à lire, produire et maintenir une documentation technique.
- La pratique de PowerShell ou d'outils d'automatisation constitue un atout.

COMPETENCES ORGANISATIONNELLES

- Capacité à analyser un incident, identifier ses causes et proposer une solution adaptée.
- Rigueur dans l'application des procédures et la traçabilité des actions.
- Aptitude à gérer les priorités dans un contexte d'activité hospitalière exigeant.
- Capacité à travailler en équipe, en autonomie et dans une organisation multi-sites.
- Sens du service aux utilisateurs et aptitude à expliquer des sujets techniques à des publics non spécialistes.
- Capacité à anticiper les risques et à contribuer à la continuité des activités.

QUALITES ATTENDUES

- Sens des responsabilités et fiabilité.
- Réactivité, disponibilité et sang-froid en situation d'incident.
- Discrétion professionnelle et respect absolu de la confidentialité.
- Curiosité technique et volonté de développer ses compétences.
- Esprit d'initiative et capacité à proposer des améliorations.
- Qualités relationnelles, pédagogie et sens du travail collectif.

7- INDICATEURS DE PERFORMANCE

- Respect des SLA
- Taux de systèmes « uptodate »
- Nombre d’audits annuels
- Taux d’application des préconisations de cybersécurité

8- STATUT, CONDITIONS DE TRAVAIL ET PARCOURS PROFESSIONNEL

Statut : Technicien supérieur hospitalier - catégorie B de la fonction publique hospitalière

Conditions de travail dans le poste :

- Horaires : statut TSH (Cf. Services RH),
- Contraintes particulières :
 - Participe aux astreintes informatiques

Formation et expérience :

- De formation supérieure Bac +2/3 en informatique
- Expérience de niveau technicien système-infra-réseau

Formation et expérience :

- Formation supérieure Bac +2 en informatique
- Expérience de niveau technicien réseaux (possibilité de premier poste)