Famille : Système d'Information	Métier : Responsable sécurité des systèmes d'information Code métier : 35I30	Quotité du poste :
Sous-famille : Expertise Systèmes d'information		Plein temps

FICHE DE POSTE :

Responsable de la Sécurité du Système d'Information et Délégué à la Protection des Données

Rédacteur(s) : Jean Michel DERU Fonction : DDOSI	Visa DRH ☐Validé	Date de validation : 03/06/2021

LOCALISATION ET RATTACHEMENT DU POSTE

LIEU D'EXERCICE

- Centre hospitalier de Blois – Département de l'organisation des systèmes d'information
- Ensemble des établissements GHT Santé 41 et des établissements membres du Lab Départemental e-Santé 41

RATTACHEMENT HIERARCHIQUE

- Directeur du Centre hospitalier de Blois

RELATIONS FONCTIONNELLES PRINCIPALES

- Directeur du département de l'organisation des systèmes d'information

DESCRIPTION DU POSTE

DEFINITION (MISSION) DU POSTE

Le poste notamment dans sa composante DPO est rattaché à la Direction générale du GHT SANTE41 composé des établissements de Blois, Romorantin-Lanthenay, Vendome, Saint Aignan, Montrichard et Selles sur Cher et des membres du Lab départemental dont le nom est « e-Santé 41 », qui a pour objectif principal de réussir la transformation numérique au niveau du département du Loir-et-Cher dont la composition est la suivante ; la Communauté professionnelle territoriale de santé (CPTS) « La Salamandre », le Groupement de coopération sociale et médico-sociale (GCSMS) « Santé Escale 41 », le Groupement de coopération sociale et médico-sociale (GCSMS) « Sepia 41 ».

ACTIVITES PRINCIPALES

Au titre de son rôle de Responsable de la Sécurité du Système d'Information

- Définition et mise à jour de la politique de sécurité des systèmes d'information :
  - Définit les objectifs et les besoins liés à la sécurité des systèmes d'information, en collaboration avec les acteurs concernés
  - Rédige la politique de sécurité des systèmes d'information et les procédures de sécurité associées en collaboration avec les acteurs concernés
  - Met en œuvre la Politique de sécurité des systèmes d'information au sein de l'établissement/des établissements parties des GHT, des membres du Lab Départemental e-Santé 41
  - Met en place une organisation permettant d'assurer, dans la durée, la gouvernance de la sécurité du système d'information des membres

- Gestion des risques :
  - Choisit une méthode d'analyse de risques adaptée à la taille et à l'activité des membres
  - Évalue les risques sur la sécurité des systèmes d'information, les menaces et les conséquences
  - Étudie les moyens permettant d'assurer la sécurité des systèmes d'information et leur bonne utilisation par les acteurs
  - Propose aux membres, pour arbitrage, une liste de mesures de sécurité à mettre en œuvre, assure dans la durée, le suivi et l'évolution de ce plan d'action et de prévention
  - Assure la maîtrise d'ouvrage de la mise en œuvre des mesures de sécurité (cette mission, selon le type de mesure technique ou organisationnelle, peut être éventuellement partagée avec un responsable métier ou la direction du système d'information

- Sensibilisation, formation et conseil sur les enjeux de la sécurité des systèmes d'information :
  - Informe régulièrement et sensibilise les directions des établissements sur les enjeux et les risques de la sécurité des systèmes d'information
  - Elabore le plan de communication et de sensibilisation relatif à la sécurité du SI auprès des acteurs en collaboration avec les partenaires
  - Conduit des actions de sensibilisation et de formation auprès des utilisateurs sur les enjeux de la sécurité des systèmes d'information
  - Participe à la réalisation de la charte de sécurité des systèmes d'information et en assure la promotion auprès de l'ensemble des utilisateurs

- Audit et contrôle de l'application des règles de la politique de sécurité des systèmes d'information :
  - Conduit régulièrement des audits de sécurité des systèmes d'information afin de vérifier la bonne application de la politique de sécurité par les acteurs de l'établissement
  - Surveille et gère les incidents de sécurité survenus au sein des établissements
  - Vérifie l'intégration de la sécurité des systèmes d'information dans l'ensemble des projets
  - Déclenche les cellules de crise en cas de sinistre Sécurité SI

- Veille technologique et prospective :
  - Suit les évolutions réglementaires et techniques afin de garantir l'adéquation de la politique de sécurité des systèmes d'information avec ces évolutions
  - Entretient et développe des réseaux de professionnels dans le domaine

Au titre de son rôle de Délégué à la Protection des Données

- Information, conseils et diffusion d'une culture de la protection des données au sein de l'établissement :
  - Mène des actions visant à sensibiliser les directions, les agents (dont le personnel participant aux opérations de traitement) aux règles à respecter en matière de protection des données à caractère personnel, s'assure que les personnes concernées sont informées des traitements opérés impliquant leurs données personnelles, ainsi que de leurs droits
  - Formalise une procédure pour informer directement le Responsable de traitement d'une non-conformité majeure. Informe sans délai le responsable de traitement de tout risque encouru en cas de non-respect de ses recommandations et de l'impact que ferait courir un risque aux directions
  - Rend compte chaque année de son action en présentant un rapport annuel aux responsables de traitement qui est le respect fidèle de son action au cours de l'année écoulée et qui fait état des éventuelles difficultés rencontrées

- Audit et contrôle du respect du règlement et du droit national en matière de protection des données :
  - Mène de façon maîtrisée et indépendante, toute action permettant de juger du degré de conformité du ou des établissements, met en évidence les éventuelles non-conformités (gravité, impacts possibles pour les personnes concernées, origine, responsabilité, etc.)
  - Vérifie le respect du cadre légal ou la bonne application de procédures, méthodes ou consignes relatives à la protection des données personnelles
  - Porte conseil auprès des directions métiers concernées et, si besoin, auprès du Responsable de traitement, ainsi qu'auprès des prestataires et sous-traitants prenant part aux traitements décidés par le responsable de traitement
  - Reçoit et traite des réclamations de personnes concernées par les traitements pour lesquels il a été désigné et veille au strict respect du droit des personnes
  - Traite les réclamations et les plaintes avec impartialité, ou met en œuvre les procédures propres à assurer leur bon traitement

- Coopération avec l'autorité de contrôle :
  - Constitue le point de contact privilégié de l'autorité de contrôle (la CNIL)
  - Etablit et maintient une documentation relative aux traitements de données à caractère personnel notamment au moyen d'un registre des traitements
  - Facilite l'accès par l'autorité aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité
  - Sollicite le conseil de l'autorité de contrôle si nécessaire

EXIGENCES DU POSTE

COMPETENCES REQUISES (ensemble des savoirs, savoir-faire et savoir-être nécessaires à la réalisation des activités du poste)

SAVOIR

- Connaissance approfondie de l'architecture SI ;
- Connaissance expert en gestion des projets ;
- Connaissance approfondie en management ;
- Connaissance approfondie en communication.

SAVOIR-FAIRE

- Connaissances approfondies de l'architecture technique du SI (serveurs, postes de travail, réseau etc)
- Connaissances approfondies de la sécurité informatique
- Connaissance du fonctionnement hospitalier et des métiers
- Connaissance du droit sur les données informatiques et médicales, de la législation, des normes, et procédures de sécurité et standards d'exploitation
- Démarche qualité, techniques d'audit : démarche d'analyse des risques (systémique, fonctionnelle etc)
- Capacité à gérer et conduire le changement, à maintenir son niveau de compétences

SAVOIR-ETRE

- Capacité d'adaptation et réactivité
- Démarche pédagogique et capacité rédactionnelle
- Sens de l'analyse, haut niveau d'objectivité et esprit de synthèse
- Rigueur, autonomie professionnelle, impartialité, capacité de prise de décision
- Ouvert et communicant, pragmatique
- Être disponible, à l'écoute et pédagogue à l'égard des utilisateurs
- Résilient, polyvalent, autonome, organisé, méthodique et rigoureux

CONNAISSANCES REQUISES

- Connaissance des concepts techniques des applications informatiques hospitalières, des réseaux informatiques et des mécanismes de sécurité.
- Connaissance des standards de sécurité ISO 2700x
- Connaissance en gestion du risque et en conformité d'un traitement à caractère personnel
- Connaissance juridique sur la sécurité des systèmes d'information, et particulièrement des textes régulant la santé
- Connaissances générales sur l'audibilité du système d'information et sur les métiers et les processus dans les hôpitaux.
- Expérience dans le pilotage de projets organisationnels dans le milieu hospitalier Appétence pour les aspects juridiques

SPECIFICITES DU POSTE ET CONDITIONS D'EXERCICE

Horaires	Sujétions ou contraintes	Autres
8h-18h		Déplacement sur tout le département Participation aux différentes réunions en lien avec ses fonctions

MOYENS MIS A DISPOSITION

DIPLÔME(S) PROFESSIONNEL(S) et FORMATION(S) REQUIS OU SOUHAITE(S)

BTS, DUT, ingénieur
Issu(e) d'une formation supérieure de niveau Bac+5, école d'ingénieur, dans le domaine informatique avec spécialisation en management des risques et sécurité des systèmes d'information.