Fiche de poste

Identification

Intitulé du poste	**Responsable de la sécurité des systèmes d'information (RSSI)**	Direction	**Logistique Systèmes d'Information**
Intitulé du métier de référence		Service	
Nom, prénom du titulaire du poste *(s'il est déjà en poste)*		Code poste SEDIT*	**06SDEC0063_PT**
		Code métier*	

Statut

Catégorie	☒ A ❑ B ❑ C	Titulaire / contractuel	
Filière	**Technique/administrative**	Cadre d'emplois	**Ingénieur / Attaché**
Grade détenu		Grades possibles	**Ingénieur/ ingénieur principal Attaché/attaché principal**

Conditions de travail

Lieu *(rattachement administratif principal)*	Hôtel du Département Angers	Travail sur écran *(+ de 2h/jour)*	❑ Non ☒ Oui
Déplacements *(lieux, fréquence…)*	❑ Non ☒ Oui	Option ARTT	❑ 1 ❑ 2 ☒ 3 ❑ Indifférent
Permis de conduire requis	❑ Non ☒Oui	Astreinte	❑ Non ❑ Oui
Matériel mis à disposition *(véhicule, tenue….)*		Délégations de signature	❑ Non ❑ Oui
Conditions de travail particulières *(travail le week-end, en soirée, travail en équipe, intempéries…)*	❑ Non ☒Oui	Lesquelles : astreintes DSI	

Prévention hygiène et sécurité : *« Il est rappelé la responsabilité de chacun en matière de respect des règles de prévention, d'hygiène et de sécurité :*

- *tout agent doit veiller à sa propre sécurité et à celle de ses collègues ;*
- *de surcroit, le manager est responsable de la bonne application de ces règles. »*

Source : Articles L4121-1 et L4122-1 du code du travail

Règles particulières d'hygiène et de sécurité à respecter [1].	☒Non ❑ Oui	Lesquelles :
Aptitudes physiques requises *(le cas échéant)*	☒ Non ❑ Oui	Lesquelles :

[1] ***En cas de réponse positive, la présente fiche de poste doit être accompagnée d'un document précisant ces règles.***

Place dans la hiérarchie et relations de travail

Fonction et nom du supérieur hiérarchique direct (N+1)	Directeur Logistique et Systèmes d'Information Cyril TOUYERAS	
Fonction des subordonnés directs (N-1) *(nombres de personnes encadrées)*		
Réalisation de l'évaluation annuelle du personnel	❑ NON	❑ OUI
Principaux interlocuteurs au sein des services départementaux	L'ensemble des agents du Département	
Principaux interlocuteurs à l'extérieur des services départementaux	Structures d'autorité (ANSSI ,…) Homologues , Constructeurs et fournisseurs de matériels/logiciels de sécurité	

Contribution du poste d'activité du Département

Missions	Au sein de la Direction Logistique et des Systèmes d'Information, sous l'autorité hiérarchique du Directeur des Systèmes d'Information le Responsable sécurité du SI évalue la vulnérabilité du système d'information de la collectivité, définit et met en œuvre la politique de sécurité de la collectivité. Il met en place des solutions et veille à leur application pour garantir la disponibilité, la sécurité et l'intégrité des données. - **Identification des risques et définition de la politique de sécurité :** - Définir et faire évoluer la politique de sécurité du système d'information, - Piloter des audits du système de sécurité, éventuellement avec l'aide de prestataires, - Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité, - Établir un plan de prévention des risques informatiques, - Définir ou faire évoluer les mesures et les normes de sécurité (charte), en cohérence avec la nature de l'activité de la collectivité et son exposition aux risques informatiques (nomadisme, BYOD, transferts de données, transactions financières...), - Proposer des dispositifs techniques appropriés aux besoins de la collectivité (outils de cryptographie, d'authentification forte ou de MFA, de corrélation d'évènements...), - Participer à la définition et au contrôle de la gestion des habilitations. - **Mise en œuvre et suivi du dispositif de sécurité :** - Faire appliquer les normes et standards de sécurité, - Mettre en place les méthodes et outils de sécurité adaptés et accompagner leur implémentation auprès des utilisateurs, - Élaborer et suivre des tableaux de bord des incidents de sécurité, - Définir les actions à mener conjointement avec les services SSIA, SRST et SPL afin de réparer les dommages causés au SI en cas de survenance d'un sinistre de sécurité SI (intrusion dans le système, contamination par un virus, défaillance d'un équipement...), mettre en œuvre le plan de reprise d'activité (PRA), - Analyser les causes des incidents et consolider les mesures de sécurité, - Tester régulièrement le bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences, - Auditer le respect des normes de sécurité informatique imposées aux sous-traitants de la collectivité. **Communication et formation sur les normes de sécurité :** - Réaliser le référentiel de sécurité, l'actualiser régulièrement, en assurer la diffusion et veiller à son application, - Définir les formations à réaliser, superviser la rédaction des supports de formation et en assurer la diffusion (principalement auprès de la DLSI), - Sensibiliser les utilisateurs aux risques de sécurité dans leur pratique de l'outil informatique par le biais de campagnes d'information, d'exercices de tentative d'hameçonnage… - Mettre en place des actions de communication (en concertation avec le responsable de l'exploitation ou les ''risk managers'' métiers) auprès des agents de la collectivité en cas de risque majeur, ou de dommages au SI, causé par une attaque ou par des dégâts matériels. - **Veille technologique et réglementaire :** - Assurer une veille technologique, de manière à garantir la sécurité logique et physique du système d'information, - Identifier les nouveaux risques sur la sécurité du système d'information : apparition de nouveaux virus, lancement d'attaques informatiques sur les réseaux, - Rechercher des solutions innovantes pour répondre aux problématiques induites par l'introduction d'une nouvelle technologie, - Suivre les évolutions juridiques du marché en termes de sécurité informatique afin de garantir la conformité du SI au droit individuel et collectif, - Rédiger des notes technologiques de sécurité. **Suivi des actions et reporting :** - Contrôler les tableaux de bord techniques des incidents de sécurité rencontrés (virus, tentatives d'intrusion...), - Assurer le reporting des problèmes de sécurité en estimant les pertes financières (pertes engendrées et coût de mise en place d'une parade).

ACTIVITES LIEES AU POSTE (10 activités maximum)	Poids relatif %	Niveau de resp[2]
> Activités principales :		
Identification des risques et définition de la politique de sécurité		II
Élaboration et suivi de la politique de sécurité		II
Mise en œuvre et suivi du dispositif de sécurité		I

Communication et formation sur les normes de sécurité		I
Veille technologique et réglementaire		I
Suivi des actions et reporting		I
> Activités secondaires :		
Encadrement/Management transverse		
Total	100 %	

[2] ***Niveau de responsabilité : I*** *- décide, est responsable de /* ***II*** *- propose, élabore, définit, participe à /* ***III*** *- exécute, met en œuvre.*

COMPETENCES LIEES AU POSTE

Savoirs (connaissances théoriques)	- Niveau Ingénieur administration réseau et télécommunications + expérience - Fondamentaux et normes relatifs à la sécurité du SI - Maîtriser les protocoles réseaux (TCP/IP), Routage …
Savoir-faire (lié à l'expérience pratique)	- Maîtriser les systèmes d'exploitations (Windows, Linux) - Maîtriser les logiciels Microsoft Exchange, Active Directory,... - Maîtriser la connectique des éléments actifs des réseaux et télécommunications - Avoir les compétences relatives aux différents matériels réseaux et leurs logiciels - Maitriser les outils de gestion de réseau DNS, WINS, Annuaires, DHCP, ... - Maîtriser l'installation de serveurs (matériels et logiciels) - Respecter les procédures d'installation, de connexion des matériels et des logiciels - Avoir une bonne expertise technique - Avoir une bonne connaissance technique et fonctionnelle des applications et services en place - Avoir une bonne connaissance du poste de travail de l'utilisateur - Posséder une expérience d'au moins 10 dans les infrastructures et notamment 2 ans dans la sécurité des systèmes d'information. - Maîtriser l'architecture fonctionnelle et technique, l'urbanisation de grands systèmes d'information, - Connaissance du domaine de la sécurité (ISO 27001, ISO 27002, ISO 27005, RGS, …), - Connaissance des infrastructures techniques de type Web, SaaS et Cloud Computing, - Connaissance des référentiels connexes RGPD, RGS, eIDAS, …
Savoir procédural (procédures)	- Connaître les normes et procédures de sécurité I&T
Savoir relationnel (relations humaines)	- Facultés d'adaptation, d'écoute et de transmission - Aisance orale et écrite
Autres	

Évolution prévisible du poste	
Document élaboré ou mis à jour le :	