WSCC Workers' Safety & Compensation Commission | ᐃᖅᑲᓇᐃᔭᖅᑎᓄᑦ ᐊᑦᑕᓇᖅᑐᓂᒃ ᐊᒻᒪ ᓇᓪᓕᐅᒃᑯᒪᓂᒃ ᖃᐅᔨᓴᖅᑎᑦ

IDENTIFICATION

Service	Titre du poste	
Commission de la sécurité au travail et de l'indemnisation des travailleurs	Spécialiste principal des systèmes de sécurité	
Numéro du poste	**Collectivité**	**Division ou région**
97-9991	Yellowknife	Rendement et services intégrés

(L'emploi du masculin pour désigner des personnes n'a d'autre fin que celle d'alléger le texte.)

OBJECTIF DU POSTE

Le spécialiste principal des systèmes de sécurité est responsable de l'analyse, de la planification, de l'élaboration, du maintien et de l'amélioration des procédures, des politiques et des mesures de gouvernance et de soutien relatives à l'architecture de sécurité de la Commission de la sécurité au travail et de l'indemnisation des travailleurs (CSTIT).

PORTÉE

La CSTIT est une société d'État des gouvernements des Territoires du Nord-Ouest (TNO) et du Nunavut qui est dirigée par un conseil d'administration (Conseil de gouvernance) par l'entremise de son président-directeur général (PDG). Elle a des bureaux situés à Yellowknife et à Iqaluit.

La CSTIT fait la promotion de la sécurité en milieu de travail par la sensibilisation et la prévention, et elle prend en charge les travailleurs blessés dans un système d'indemnisation sans égard à la faute. Ce système est financé par des cotisations d'employeurs et est régi par les *Lois sur l'indemnisation des travailleurs* des TNO et du Nunavut.

La CSTIT est résolue à offrir un environnement exempt de racisme et de discrimination, où tous et toutes se sentent en sécurité dans la prestation et la réception de services. Cet objectif peut être atteint par un engagement respectueux à reconnaître l'importance des différences culturelles et à valoriser la sécurisation culturelle.

L'infrastructure de technologie de l'information de la CSTIT, essentielle au bon déroulement des opérations, s'étend sur plusieurs bureaux et territoires et répond à diverses exigences en matière de données. Dotée d'un budget annuel de plus de 5 millions de dollars, elle met en relief la nécessité d'une performance et d'une fiabilité élevées et continues, compte tenu de la complexité du réseau à l'échelle territoriale.

Exerçant ses fonctions à Yellowknife, le spécialiste principal des systèmes de sécurité (spécialiste) relève du gestionnaire des technologies de l'information et de l'informatique décisionnelle. Il est appelé à fournir des services spécialisés aux employés actifs de la CSTIT à Yellowknife et à Iqaluit.

Le titulaire du poste doit procéder à l'analyse complète, à la planification, à l'élaboration, au maintien et à l'amélioration de tous les processus et politiques en matière de gouvernance et de sécurité, ainsi qu'à la mise en œuvre de l'infrastructure de sécurité. Ses tâches consistent notamment à contribuer à l'élaboration de politiques, de procédures, de normes et de lignes directrices relatives à la sécurité de l'information qui régissent la gestion de l'information (GI), les systèmes d'information (SI) et les technologies de l'information (TI). Ce spécialiste devra établir une base de référence en matière de sécurité de l'information au sein de la CSTIT et consulter les divisions afin de comprendre leurs fonctions opérationnelles et d'interpréter leur propension et leur tolérance au risque en vue de les traduire en un état futur souhaité et réalisable.

Le titulaire du poste travaillera directement à la mise en œuvre de mesures de sécurité axées sur l'infrastructure ou les applications. Cependant, il travaillera en étroite collaboration avec les équipes des divisions chargées de la maintenance de ces actifs afin de s'assurer qu'elles comprennent les exigences à respecter. De plus, il fournira des directives et des conseils quant aux pratiques exemplaires afin de garantir la mise en œuvre la plus efficace possible des mesures liées à la sécurité de l'information. Il sera chargé de diriger l'élaboration du cadre d'intervention à suivre lors d'incidents et dans le cadre d'enquêtes de la CSTIT, assurant ainsi une gestion rapide et efficace des incidents de sécurité. Il lui incombera également de gérer et de mener des évaluations complètes de cas en matière de sécurité, de mettre en place des formations centrées sur la sensibilisation et de veiller au respect des normes afin de renforcer la résilience de l'organisation en matière de cybersécurité.

En tant que membre de l'équipe des Services d'information, le spécialiste est tenu d'interagir professionnellement avec les clients dans toutes les situations. Possédant une expertise en sécurité et en administration des systèmes, il contribue à la mise en œuvre du plan stratégique des Services d'information et contribue aux initiatives liées à ce plan.
Le titulaire du poste doit composer avec des incidents de service susceptibles d'avoir d'importantes répercussions sur le fonctionnement de la CSTIT et, par conséquent, de nécessiter une intervention rapide et une reprise du service. Ces incidents peuvent survenir à tout moment, 24 heures sur 24, 365 jours par année. Le titulaire du poste peut devoir intervenir sur appel pendant de longues périodes ou par rotation, tous les jours et à toute heure, pour assurer la fiabilité du réseau.
Ce poste peut exiger de son titulaire qu'il travaille selon des horaires variables pour soutenir les régions. Des déplacements dans les communautés régionales seront nécessaires de temps à autre.

- Soutenir les activités liées aux responsabilités énoncées ci-dessus

RESPONSABILITÉS

1. **Assurer un niveau élevé de leadership dans l'administration de la sécurité pour tous les utilisateurs à l'intérieur et à l'extérieur du réseau de la CSTIT**
    - Veiller au respect des procédures d'administration de la sécurité afin de sécuriser les serveurs et les systèmes de stockage de la CSTIT pour tous les utilisateurs à l'intérieur et à l'extérieur du réseau de celle-ci
    - Établir et appliquer des normes pour assurer la sécurité des serveurs, du stockage et du réseau, veiller à leur maintenance, contrôler l'accès et faire respecter les procédures en place
    - Concevoir et mettre en œuvre un accès contrôlé aux données pour les entités externes sans compromettre l'intégrité et la sécurité des dépôts de données de la CSTIT

- Gérer les processus et protocoles de sécurité, en garantissant un accès sécurisé des applications aux systèmes de données, au courrier électronique et aux applications distantes
- Se tenir au courant des avancées technologiques dans le domaine de la gestion des serveurs et du stockage, et contribuer ainsi aux décisions visant à améliorer la sécurité, le rendement, la stabilité et la prise en charge
- Diriger les opérations de maintenance des systèmes de sécurité
- Enquêter sur les infractions à la sécurité et veiller à leur résolution
- S'acquitter de tâches d'administration de la sécurité normalisées et non normalisées, en veillant à résoudre les problèmes de sécurité
- Collaborer avec le gestionnaire des technologies de l'information, le spécialiste principal des serveurs et des réseaux, d'autres collègues de la CSTIT et des entrepreneurs pour mettre en œuvre et soutenir les procédures de sécurité du réseau

2. Diriger et mettre en œuvre des mesures de gouvernance en matière de sécurité

- Participer à l'exploitation des technologies de sécurité de l'information, y compris, mais sans s'y limiter, les systèmes de prévention et de détection des intrusions sur le réseau, des systèmes antivirus organisationnels, les systèmes organisationnels de prévention des intrusions d'hôte, les pare-feu, les systèmes de gestion des correctifs, le chiffrement de bout-en-bout, la protection ponctuelle et les systèmes de gestion des incidents de sécurité
- Diriger les mesures d'intervention lors d'incidents de sécurité : coordonner les efforts de récupération et de reprise des activités, diffuser l'information auprès des intervenants et travailler avec des consultants en réponse aux incidents
- Travailler en étroite collaboration avec l'analyste principal des serveurs et des réseaux au sein de l'équipe des technologies de l'information pour assurer la sécurité de l'infrastructure technologique de la CSTIT
- Diriger la création et l'application des politiques, procédures, normes et directives ainsi que des plans connexes pour assurer la sécurité de l'information et mettre en place des contrôles d'accès conformément aux pratiques exemplaires de l'industrie et aux directives en matière de gestion
- Aider l'équipe des technologies de l'information à créer et à examiner les plans de reprise après sinistre et de continuité des activités en cas de perte de technologies ou d'applications opérationnelles
- Mener des examens de sécurité, des évaluations de vulnérabilité, des essais de pénétration et des évaluations des risques de l'infrastructure ou des systèmes – en coordination avec un consultant ou un cabinet externe spécialisé en services de sécurité professionnelle, s'il y a lieu
- Offrir des programmes de formation et de sensibilisation dans le domaine de la sécurité de l'information ou collaborer avec le gestionnaire des technologies de l'information ou un consultant pour en offrir dans l'ensemble de la CSTIT

3. Fournir une expertise et un soutien dans la configuration, le déploiement et la maintenance de réseaux complexes

- Évaluer, planifier et déployer une infrastructure de réseau afin de garantir une connectivité transparente et un rendement optimal au sein des services et des équipes de la CSTIT
- Collaborer avec des intervenants pour définir les exigences du réseau, en proposant des recommandations éclairées
- Procéder au dépannage et à la résolution de problèmes complexes liés au réseau, en coordination avec les équipes compétentes
- Concevoir et mettre en œuvre des mesures et des protocoles de sécurité pour le réseau
- Diriger l'élaboration de la documentation relative au réseau et en assurer la mise à jour exhaustive

- Rester au courant des avancées technologiques en matière d'infrastructure réseau, et contribuer ainsi à la prise de décisions stratégiques pour assurer la performance optimale du réseau
- Collaborer avec l'équipe élargie de la CSTIT et les partenaires externes pour améliorer les services de réseau

4. Participer aux vérifications périodiques officielles et aux examens des jalons

- Garantir le maintien de l'intégrité globale, de la sécurité et de l'accessibilité des données
- Maintenir un niveau constamment élevé en matière de documentation et y contribuer
- Aider à la préparation des rapports, à la formulation de recommandations ou à la recherche de solutions de rechange pour régler des aspects qui posent des problèmes ou risquent de le faire dans les systèmes d'exploitation
- Préparer des modèles de système, devis, diagrammes et graphiques pour offrir des orientations aux responsables internes et contractuels du développement
- Veiller à ce que les normes de service soient respectées dans les solutions opérationnelles

CONDITIONS DE TRAVAIL

Exigences physiques

Aucune exigence inhabituelle

Conditions environnementales

Aucune condition inhabituelle

Exigences sensorielles

Aucune exigence inhabituelle

Exigences mentales

Aucune exigence inhabituelle

CONNAISSANCES, APTITUDES ET HABILETÉS

- Une connaissance de l'administration de la sécurité des systèmes, ainsi que des pratiques et procédures en matière de sécurité de l'information
- Une connaissance des pare-feu, des systèmes de prévention et de détection des intrusions, des logiciels antivirus organisationnels et des systèmes organisationnels de gestion des correctifs
- Une connaissance des pratiques exemplaires en matière de sécurité de l'information dans le cadre du développement d'applications logicielles personnalisées
- Une connaissance de la législation sur la sécurité de l'information et la protection des renseignements personnels dans un contexte canadien
- Une connaissance des protocoles courants tels que TCP/IP, SNMP, HTTP et Radius ainsi qu'une connaissance approfondie des technologies et protocoles de cryptographie, y compris Kerberos, PKI et AES/DES
- Une connaissance des cycles de développement des systèmes (CDS) et des moyens d'intégrer les pratiques exemplaires en matière de sécurité de l'information dans un CDS
- Des compétences relatives aux systèmes de prévention et de détection des intrusions sur le réseau, aux systèmes antivirus organisationnels, aux systèmes organisationnels de prévention des intrusions d'hôte, aux pare-feu, aux systèmes de gestion des correctifs, au chiffrement de bout-en-bout, à la protection ponctuelle et aux systèmes de gestion des incidents de sécurité

- Des compétences et des connaissances relatives aux systèmes de gestion de la sécurité de l'information, aux cadres de contrôle (COBIT, ISO 27001, NIST CSF) et aux méthodologies d'évaluation des risques connexes (CIS, PCI, HIPPA, HIA, etc.)
- Des aptitudes pour l'analyse et la résolution de problèmes
- La capacité de mener des recherches sur des problèmes et des produits de sécurité, au besoin
- La capacité d'évaluer, de planifier et de déployer une infrastructure de réseau afin de garantir une connectivité transparente et un rendement optimal au sein des services et des équipes de la CSTIT
- Des compétences en matière de relations interpersonnelles, de communications et d'organisation
- Le souci du détail et de la précision
- La capacité de négocier, de persuader et de trouver un compromis entre les intervenants
- La capacité de se perfectionner sur le plan professionnel pour toujours mieux répondre aux besoins de la CSTIT en matière de sécurité
- La capacité de rester calme et concentré dans les situations difficiles
- Un engagement à défendre activement et à respecter soi-même de manière cohérente la diversité personnelle, l'inclusion et la sensibilisation aux cultures, ainsi que les différentes approches en matière de sécurité et de sécurisation culturelle au travail

Généralement, les qualifications ci-dessus seraient acquises par :

Un diplôme en génie, en informatique, en cybersécurité, en technologie de l'information ou en gestion de l'information et une expérience pertinente de quatre (4) ans, dont deux (2) dans le domaine de la sécurité de l'information ou des réseaux

Toute combinaison équivalente de formation et d'expérience sera prise en considération.

EXIGENCES SUPPLÉMENTAIRES

Niveau de sécurité

☐ Aucune vérification du casier judiciaire requise

☒ Poste de confiance – vérification du casier judiciaire exigée

☐ Poste donnant accès à des renseignements de nature délicate – vérification de l'identité et du casier judiciaire exigée

Langue française (cocher une seule case)

☐ Français requis (indiquer le niveau ci-dessous)

Le niveau requis pour le poste désigné est :

EXPRESSION ORALE ET COMPRÉHENSION

De base (B) ☐ Intermédiaire (I) ☐ Avancé (A) ☐

COMPRÉHENSION EN LECTURE

De base (B) ☐ Intermédiaire (I) ☐ Avancé (A) ☐

COMPÉTENCES EN RÉDACTION

De base (B) ☐ Intermédiaire (I) ☐ Avancé (A) ☐

☐ Français de préférence

Langues autochtones : Pour choisir une langue, cliquer ici.

☐ Requis ☒ De préférence