



La Haute Ecole Léonard de Vinci asbl (HE Vinci)

Recherche un conseiller en sécurité de l'information (H/F)

Contrat à durée déterminée à temps plein

Entrée en fonction : immédiate

La Haute Ecole Vinci organise 42 formations dispensées au sein de 5 instituts : l'ECAM, l'Ecole Normale Catholique du Brabant wallon, l'institut libre Marie Haps, l'institut Paul Lambin et le PARNASSE-ISEI. Elle emploie plus de 1000 travailleurs et compte plus de 8000 étudiants sur les sites de Bruxelles et Louvain-la-Neuve. A travers ses instituts, elle est en outre active dans la recherche, dans la formation continue et dans de nombreux services à la société.

Missions du conseiller en sécurité de l'information

La mission du conseiller en sécurité de l'information est de sécuriser les actifs numériques, les données et les systèmes de la HE Vinci et de s'assurer que ceux-ci répondent aux exigences légales concernant la sécurité et la protection de la vie privée.

Le conseiller en sécurité de l'information remet ses avis en toute indépendance. Il dispose d'un positionnement transversal dans la structure de la Haute Ecole. Il rapporte directement au Directeur-président.

En termes de prévention :

Le conseiller en sécurité de l'information est chargé de :

- définir, maintenir et mettre à niveau une politique de sécurité de l'information entre les différentes entités de la Haute Ecole et s'assurer de l'application de cette politique dans les différents domaines (courrier électronique, hébergement web, réseaux sociaux, applications web et bureautiques, bases de données, stockage dans le cloud, ...).
- élaborer et entretenir des procédures relatives à la sécurité de l'information, qu'elles soient générales ou destinées à des groupes cibles et/ou pour certains systèmes d'information.
- élaborer un plan de sécurité à 3 ans.
- procéder chaque année à l'évaluation, à la rédaction de rapports obligatoires et à l'adaptation du plan de sécurité.
- veiller à ce que les incidents et infractions de sécurité affectant les systèmes d'information fassent l'objet d'une analyse en termes de risques actuels et futurs et rapporter les infractions constatées, accompagnées des avis nécessaires.

En termes de gestion :

Dans le cadre des activités quotidiennes du système informatique, le conseiller en sécurité de l'information est chargé de :

- gérer les incidents liés au non-respect des réglementations en matière de protection des données personnelles ou liés à des failles de sécurité résultant de mauvaises configurations ou de mauvaises pratiques de programmation.
- gérer les incidents liés à des incohérences de données et imprécisions d'encodage.
- gérer les incidents de hacking, phishing, intrusions, ...
- réaliser une veille technologique et réglementaire en matière de sécurité de l'information ainsi que tenir en permanence à jour ses connaissances en matière de sécurité de l'information.
- tenir le registre des activités de traitements applicable à la Haute école.
- développer la sensibilisation et promouvoir le respect des règles de sécurité ainsi que l'adoption d'un comportement favorisant la sécurité.
- coordonner la certification et l'homologation des systèmes d'information traitant des informations classifiées.
- définir clairement les différentes responsabilités sur le plan de la sécurité (prévention, contrôle, détection et traitement).
- formuler des recommandations et apporter des améliorations en matière de sécurité de l'information.
- veiller à la sécurisation logique et physique des données afin de garantir la sécurité quotidienne de l'échange de données relatives à la vie privée.
- travailler en étroite collaboration avec d'autres services, informatiques ou autres et notamment avec le Data Protection Officer de la HE Vinci.

Qualifications et aptitudes requises

- Master (diplôme universitaire ou équivalent dans un des domaines suivants : sciences juridiques, sciences économique et de gestion, sciences de l'ingénieur et technologies, master en sécurité informatique ou diplôme de bachelier des mêmes domaines, complété par une expérience probante ou une formation complémentaire en audit et sécurité).
- Une expérience en gestion d'infrastructure informatique et de leur sécurité, dans des environnements de grande échelle.
- Une connaissance approfondie des protocoles réseaux courants (TCP/IP, ...)
- Une expertise technique en sécurité « infrastructures » : FW-NG, VPN, IPS, IDS, ...
- Une expertise technique en sécurité « services » : serveurs et applications web, mails, ...
- Des compétences dans les techniques et méthodes de développement d'applications fiables et sécurisées
- Rigueur dans la rédaction des procédures et de la documentation.

- Aptitude à travailler seul et en équipe, à communiquer et à partager l'information.
- Autonomie et sens des responsabilités
- Sens irréprochable de la confidentialité.

Conditions d'engagement

Nous vous offrons un contrat de travail à durée déterminée à temps plein (38h), dans un cadre de travail agréable et dynamique situé à proximité des voies de communication et transports publics ; régime de congé attractif, reconnaissance de l'expérience professionnelle et formation continuée.

Procédure de sélection

La sélection est organisée en trois étapes :

1. analyse des dossiers de candidatures où les critères énoncés dans l'appel d'offre sont vérifiés ;
2. épreuve technique afin de pouvoir confronter les candidats aux compétences attendues pour cette fonction ;
3. rencontre des candidats par une commission de recrutement.

Procédure de dépôt de candidature

Les candidatures accompagnées d'un curriculum vitae et d'une lettre de motivation sont à envoyer par mail à Madame Houria ZARKI à l'adresse houria.zarki@vinci.be AVANT le 20 mai 2019.