|  |  |
| --- | --- |
| Logo of the European Commission, 12 yellow stars on a blue background arranged in a circle and framed by two light grey graphic elements representing the Berlaymont building, which is the headquarter of the European Commission. | COMMISSION EUROPÉENNE |

AVIS DE VACANCE POUR UN POSTE D’EXPERT NATIONAL DÉTACHÉ

|  |  |
| --- | --- |
| DG – Direction – Unité | DIGIT.S.1 |
| Numéro de poste Sysper: | 288740 |
| Personne de contact:  Prise de fonctions souhaitée:  Durée initiale:  Lieu de détachement: | Renaat LEURIDAN  4ème trimestre 2023  … années  Bruxelles  Luxembourg  Autre: Click or tap here to enter text. |
| Type de détachement |  |
| Cet avis de vacance est ouvert aux:    ainsi qu’aux  pays AELE suivants:  Islande  Liechtenstein  Norvège  Suisse  pays tiers suivants: …  organisations intergouvernementales suivantes: … | |
| Délai des candidatures |  |

**Présentation de l’entité (nous sommes)**

DIGIT est le service informatique central de la Commission, avec pour mission de fournir des services numériques permettant la mise en œuvre des politiques de l'UE et de soutenir les processus internes et l'administration de la Commission. DIGIT est, entre autres, responsable de l'infrastructure réseau à travers la Commission, des centres de données centraux au Luxembourg, de près de 50 000 postes de travail d'utilisateurs finaux et d'un grand nombre de systèmes d'information soutenant les processus métiers de la Commission.

La direction S (sécurité informatique) est une direction de DIGIT, créée le 1er janvier 2016. L'unité S1 (politique de sécurité informatique) est basée à Bruxelles et est chargée de définir la politique et la stratégie de sécurité informatique à l'échelle de la Commission, en soutenant les propriétaires de systèmes en matière de sécurité informatique, l'évaluation des risques, la création de plans de sécurité informatique pour les systèmes critiques et la vérification de la conformité technique des systèmes une fois qu'ils sont déployés (par exemple, la recherche de vulnérabilités). L'unité S2 est responsable de la surveillance des systèmes et de la détection et de la réponse aux incidents de sécurité informatique.

L'équipe politique de l'unité S1 est responsable de l'élaboration de la stratégie de sécurité informatique à l'échelle de la Commission et de la politique de sécurité informatique (y compris les normes et lignes directrices spécifiques). Pour cette tâche, l'équipe chargée de la politique travaille en étroite collaboration avec divers interlocuteurs clefs de la Commission, en particulier avec le réseau de responsables locaux de la sécurité informatique dans l'ensemble de la Commission, avec des experts en sécurité informatique au sein du service informatique de la Commission (appelé DIGIT), des groupes de travail d'experts en informatique et avec le comité directeur incluant le domaine de la sécurité de l'information.

**Présentation du poste (nous proposons)**

Cet avis de vacance vise à recruter un(e) END en tant que responsable de la politique de sécurité informatique au sein de l'équipe politique de l'unité S1. Les principales tâches du responsable de la politique de sécurité informatique consistent à élaborer la stratégie de sécurité informatique et la politique de sécurité informatique, en étroite collaboration avec les différentes parties prenantes de DIGIT, dans d'autres directions générales de la Commission, en particulier la DG HR, la DG CNECT et les organismes comme le CERT-EU et l'ENISA.

Les tâches et responsabilités du responsable de la politique de sécurité informatique comprendront :

* Gérer et soutenir une transition de la politique, des règles et des normes existantes vers une configuration plus moderne, qui se concentre davantage sur les risques et moins sur le respect des règles.
* Mettre en place un processus pour examiner l'efficience et l'efficacité des politiques, règles et normes, en tenant compte des nouvelles menaces, des incidents passés, des changements dans l'appétence au risque, des nouvelles technologies, des nouveaux besoins commerciaux, etc.
* Identifier les domaines dans lesquels de nouvelles normes ou directives sont nécessaires et travailler avec les interlocuteurs clefs de la DIGIT pour collecter, développer et mettre ces normes et directives à la disposition de l’audience concernée (utilisateurs finaux, propriétaires de systèmes, experts, développeurs, etc.).
* Mettre en place un processus de gouvernance de la sécurité informatique pour fournir à la direction générale et aux responsables locaux de la sécurité informatique des informations exploitables sur la sécurité informatique (risques, incidents, mesures en place, conformité technique, etc. ).
* Identifier les domaines d'amélioration et travailler avec les interlocuteurs clefs de la Commission pour définir des projets et des activités, et consolider ces améliorations dans une stratégie à l'échelle de la Commission.
* Développer et maintenir les outils informatiques de support à la gestion du risque et de la conformité utilisant la technologie ServiceNow.

**Profil du titulaire (nous recherchons)**

Critères d’éligibilité

Expérience professionnelle : au moins trois ans d'expérience dans des fonctions administratives, juridiques, scientifiques, techniques, de conseil ou d'encadrement, dans le domaine de l'informatique et/ou de la cyber-sécurité, pouvant être considérées comme équivalentes à celles des groupes de fonctions AD ;

Critères de sélection

- diplôme

Diplôme universitaire sanctionnant des études universitaires accomplies d'une durée d'au moins 3 ans dans le domaine des TIC ou un domaine connexe (tel que informatique, ingénierie, physique, informatique métiers, droit de l'informatique), justifié par le cursus et/ou les options de spécialisation correspondants dans lequel le candidat a obtenu son diplôme.

- expérience professionnelle :

Bonne connaissance des normes, des cadres et des méthodologies de sécurité de l'information et de gestion des risques informatiques, tels que ISO 27001 ou COBIT.

Au moins 3 ans d'expérience pratique dans le domaine de la définition et de la mise en œuvre de stratégies de sécurité de l'information, de cadres de sécurité informatique et/ou de programmes de gestion des risques ; compréhension des défis associés aux environnements d'entreprise / gouvernementaux / d'administration publique.

Bonnes capacités de communication et de présentation.

Expérience dans la gestion des relations avec les parties prenantes.

Forte capacité à apprendre et à appliquer de nouvelles méthodes de travail, concepts et méthodologies.

- compétences optionnelles (pourraient être un avantage) :

Bonne compréhension de l'infrastructure informatique et des réseaux

Bonne compréhension des technologies et processus de sécurité informatique

Compréhension des cadres de conformité Cloud Computing et de cybersécurité

Expérience en ServiceNow

Expérience en outils GRC (gouvernance, risque et conformité)

Si vous répondez aux critères ci-dessus, votre passion est votre guide, le respect et le travail d'équipe sont pour vous un must absolu et vous avez une attitude "can do", votre candidature est la bienvenue.

- langue(s) nécessaire(s) pour l'exercice des fonctions :

Anglais : courant écrit et parlé requis

Français : pourrait être un avantage

**Critères d’éligibilité**

Le détachement sera régi par la **décision de la Commission C(2008) 6866** du 12/11/2008 relative au régime applicable aux experts nationaux détachés et aux experts nationaux en formation professionnelle auprès des services de la Commission (décision END).

Aux termes de la décision END, vous devrez obligatoirement remplir les critères d’éligibilité suivants **à la date de début du détachement** :

Expérience professionnelle : posséder une expérience professionnelle d’au moins trois ans dans des fonctions administratives, judiciaires, scientifiques, techniques, de conseil ou de supervision, à un grade équivalant au groupe de fonctions administrateur AD;

Ancienneté de service : avoir une ancienneté d’au moins un an (12 mois) auprès de votre employeur actuel, dans un cadre statutaire ou contractuel;

Employeur : être employé par une administration publique nationale, régionale ou locale, ou par une organisation intergouvernementale (OIG); exceptionnellement et après dérogation, la Commission peut accepter des candidatures lorsque votre employeur est un organisme du secteur public (e.g. agence ou institut de régularisation), une université ou un organisme de recherche indépendant.

Compétences linguistiques : avoir une connaissance approfondie d’une des langues de l’Union européenne et une connaissance satisfaisante d’une autre langue de l’Union européenne dans la mesure nécessaire aux fonctions qu’il est appelé à exercer. Si vous venez d’un pays tiers, vous devrez justifier posséder une connaissance approfondie de la langue de l’Union européenne nécessaire à l’accomplissement des tâches qui vous seront confiées.

**Conditions du détachement**

Durant toute la durée de votre détachement, vous devrez rester employé et rémunéré par votre employeur et devrez également rester couvert par votre sécurité sociale (nationale).

Vous exercerez vos fonctions au sein de la Commission dans les conditions fixées par la décision END précitée et serez soumis(e) aux règles de confidentialité, de loyauté et d’absence de conflit d’intérêts qui y sont définies.

Dans le cas où le poste est publié avec indemnités de séjour, celles-ci ne vous seront octroyées que si vous remplissez les conditions prévues à l’article 17 de la décision END.

Le personnel en poste dans une délégation de l’Union européenne doit obligatoirement disposer d’une habilitation de sécurité (jusqu’au niveau SECRET UE/EU SECRET conformément [à la décision de la Commission (EU – Euratom) 2015/444 du 13 mars 2015](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32015D0444). Il vous appartient de lancer cette procédure d’habilitation de sécurité avant d’obtenir la confirmation de votre détachement.

**Soumission des candidatures et procédure de sélection**

Si vous êtes intéressé, veuillez suivre les instructions données par votre employeur pour postuler.

La Commission Européenne **acceptera seulement les candidatures qui auront été soumises par l’intermédiaire de la Représentation Permanente / Mission Diplomatique de votre pays auprès de UE, le secrétariat de l’AELE (EFTA) ou par le(s) canal (canaux) qui aura (auront) été spécifiquement convenu(s)**. Les candidatures reçues directement de votre part ou de votre employeur ne seront pas prises en considération.

Vous devez envoyer votre candidaturesous format **CV Europass** ([Créez votre CV Europass | Europass](https://europa.eu/europass/fr/create-your-europass-cv))en français, anglais ou allemand.Votre CV doit obligatoirement mentionner votre nationalité.

Veuillez ne pas ajouter d’autres documents(tels que copie de carte d’identité, copie des diplômes ou attestation d’expérience professionnelle, etc.). Le cas échéant, ces documents vous seront demandés ultérieurement.

**Traitement des données à caractère personnel**

La Commission européenne veillera à ce que les données à caractère personnel des candidats soient traitées dans le plein respect du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([[1]](#footnote-1)). Ces dispositions s’appliquent en particulier à la confidentialité et à la sécurité de ces données. Avant de postuler, veuillez lire la déclaration de confidentialité.

1. () Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel par les institutions, organes et organismes de l’Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39). [↑](#footnote-ref-1)