|  |  |
| --- | --- |
| 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. | EUROPEAN COMMISSION |

VACANCY NOTICE FOR A POST OF SECONDED NATIONAL EXPERT

|  |  |
| --- | --- |
| DG – Directorate – Unit | DIGIT.S.1 |
| Post number in sysper: | 288740 |
| Contact person:Provisional starting date:Initial duration:Place of secondment: | Renaat LEURIDAN4th quarter 2023… years[x]  Brussels [ ]  Luxemburg [ ]  Other:  |
| Type of secondment |  |
| This vacancy notice is open to:as well as[ ]  The following EFTA countries: [ ]  Iceland [ ]  Liechtenstein [ ]  Norway [ ]  Switzerland[ ]  The following third countries: …. [ ]  The following intergovernmental organisations: …   |
| Deadline for applications |  |

**Entity Presentation (We are)**

DIGIT is the central IT department of the Commission, with a mission to deliver digital services to enable the implementation of EU policies and support the Commission's internal processes and administration. DIGIT is, among other things, responsible for the network infrastructure across the Commission, the central datacentres in Luxembourg, close to 50.000 end-user workstations, and a large number of information systems supporting business processes in the Commission.

Directorate S (Cybersecurity) is a directorate in DIGIT, created on January 1st 2016. Unit S1 (IT Security Policy) is based in Brussels and is responsible for defining the Commission wide IT security policy and strategy, supporting system owners with IT security risk assessments, the creation of IT security plans for critical systems, and to check the technical compliance of systems once they are deployed (e.g. scanning for vulnerabilities). Unit S2 is responsible for the monitoring of systems and the detection of and response to IT security incidents.

The policy team in unit S1 is responsible for developing the Commission wide IT security strategy and the IT security policy (including specific standards and guidelines). For this task the Policy team works closely with various stakeholders in the Commission, particularly with a network of local IT security officers across the Commission, with IT security experts inside the Commission's IT department (called DIGIT), working groups of IT experts, and with senior management represented in a high-level steering board for information security.

**Job Presentation (We propose)**

This vacancy notice is to recruit an SNE to work as IT security policy officer in the Policy team in unit S1. The main tasks of the IT Security policy officer is to develop the IT security strategy and the IT security policy, working closely together with the different stakeholders in DIGIT, in other Directorate Generals of the Commission, in particular DG HR, DG CNECT, and bodies like CERT-EU and ENISA.

The tasks and responsibilities of the IT Security Policy Officer will include:

* Managing and supporting a transition from the existing policy, rules and standards to a more modern setup, which focuses more on risks and less on compliance with rules.
* Setting up a process to review the efficiency and effectiveness of policy, rules and standards, taking into account new threats, past incidents, changes in risk appetite, new technology, new business needs, et cetera.
* Identifying areas where new standards or guidelines are needed, and work with stakeholders across DIGIT to collect, develop, and make these standards and guidelines available to the relevant audience (end-users, system owners, experts, developers, etc).
* Setting up an IT security governance process to provide senior management and local IT security officers with actionable information about IT security (risks, incidents, measures in place, technical compliance, etc. ).
* Identifying areas for improvement and working with stakeholders across the Commission to define projects and activities, and consolidating these improvements in a Commission wide strategy.
* Setting up a process to provide senior management and local IT security officers with information about the implementation of the IT security strategy.
* Build and maintain IT support tooling for Risk and Compliance management based on ServiceNow technology.

**Jobholder Profile (We look for)**

Eligibility criteria

Professional experience: at least three years' experience in administrative, legal, scientific, technical, advisory or supervisory functions, in the domain of IT and/or in cybersecurity, which can be regarded as equivalent to those of function groups AD.

Selection Criteria

- diploma:

University diploma certifying completed university studies of the duration of at least 3 years in the field of ICT or an associated field (such as computer studies, engineering, physics, IT business, IT law), proven by the corresponding curriculum and/or specialisation options in which the candidate graduated.

- professional experience:

Good knowledge of information security and IT risk management standards, frameworks and methodologies, such as ISO 27001 or COBIT.

At least 3 years of practical experience in the domain of definition and implementation of information security strategies, IT security frameworks and/or risk management programmes; understanding of the challenges associated with corporate / governmental / public administration environments.

Good communication and presentation skills.

Experience in stakeholders’ relationship management.

Strong ability to learn and apply new ways of working, concepts and methodologies.

- optional skills (is an advantage):

Good understanding of IT infrastructure and networking

Good understanding of IT security technology and processes

Understanding of Cloud Computing and cybersecurity cloud compliance frameworks

Service Now technology experience

GRC tooling experience (Governance, Risk and Compliance)

If you meet the above criteria, your passion is your driver, respect and teamwork are an absolute must for you and you have a "can do" attitude, your application is welcome.

- language(s) necessary for the performance of duties:

English: fluent written and spoken required

French: could be an advantage

**Eligibility criteria**

The secondment will be governed by the **Commission Decision C(2008) 6866** of 12/11/2008 laying down rules on the secondment to the Commission of national experts and national experts in professional training (SNE Decision).

Under the terms of the SNE Decision, you need to comply with the following eligibility criteria at **the starting date** of the secondment:

* Professional experience: at least three years of professional experience in administrative, legal, scientific, technical, advisory or supervisory functions which are equivalent to those of function group AD.
* Seniority: having worked for at least one full year (12 months) with your current employer on a permanent or contract basis.
* Employer: must be a national, regional or local administration or an intergovernmental public organisation (IGO); exceptionally and following a specific derogation, the Commission may accept applications where your employer is a public sector body (e.g., an agency or regulatory institute), university or independent research institute.
* Linguistic skills: thorough knowledge of one of the EU languages and a satisfactory knowledge of another EU language to the extent necessary for the performance of the duties. If you come from a third country, you must produce evidence of a thorough knowledge of the EU language necessary for the performance of his duties.

**Conditions of secondment**

During the full duration of your secondment, you must remain employed and remunerated by your employer and covered by your (national) social security system.

You shall exercise your duties within the Commission under the conditions as set out by aforementioned SNE Decision and be subject to the rules on confidentiality, loyalty and absence of conflict of interest as defined therein.

In case the position is published with allowances, these can only be granted when you fulfil the conditions provided for in Article 17 of the SNE decision.

Staff posted in a European Union Delegation are required to have a security clearance (up to SECRET UE/EU SECRET level according to [Commission Decision (EU, Euratom) 2015/444 of 13 March 2015](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015D0444). It is up to you to launch the vetting procedure before getting the secondment confirmation.

**Submission of applications and selection procedure**

If you are interested, please follow the instructions given by your employer on how to apply.

The European Commission **only accepts applications which have been submitted through the Permanent Representation / Diplomatic Mission to the EU of your country, the EFTA Secretariat or through the channel(s) it has specifically agreed to**. Applications received directly from you or your employer will not be taken into consideration.

You should draft you CV in English, French or German using the **Europass CV format** ([[Create your Europass CV | Europass](https://europa.eu/europass/en/create-europass-cv)](http://europass.cedefop.europa.eu/en/documents/curriculum-vitae)). It must mention your nationality.

Please do not add any other documents(such as copy of passport, copy of degrees or certificate of professional experience, etc.). If necessary, these will be requested at a later stage.

**Processing of personal data**

The Commission will ensure that candidates’ personal data are processed as required by Regulation (EU) 2018/1725 of the European Parliament and of the Council ([[1]](#footnote-1)). This applies in particular to the confidentiality and security of such data. Before applying, please read the attached privacy statement.

1. () Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39 [↑](#footnote-ref-1)