

INTERNAL VACANCY NOTICE – Security Officer (Information Security and Assurance Sector & Cyber Security Sector profiles) (AD5)

Ref. eu-LISA/25/TA/AD5/6.2



Sector and Unit	Information Security & Assurance Sector and Cyber Security Sector / Security Unit
Grade bracket	AD5-AD7 (Temporary Staff)
Place of Employment	Strasbourg (France) and Tallinn (Estonia)
Working model	Hybrid working arrangements – Permanent relocation required
<u>Level of Security Clearance</u>	SECRET UE/EU SECRET
Deadline for Application	11 March 2025 ¹ Extended until 31 March 2025 at 12:59 pm Tallinn time/ 11:59 am Strasbourg time
Validity of the Reserve List	31 December 2028

About the unit

The Security Unit (SCU) is responsible for safeguarding eu-LISA's assets, in particular the large-scale IT systems and data entrusted to the Agency. By ensuring the secure and continuous operation of large-scale IT systems, together with an appropriate level of data and physical security, SCU contributes to compliance with the provisions of Article 2 of eu-LISA's establishing Regulation.

To ensure uninterrupted service availability to the EU's JHA community, SCU's scope of activities covers security governance and assurance, risk management, information security, business continuity and disaster recovery. This task includes overseeing eu-LISA's security and continuity management system (SCMS) and operating the Computer Security Incident Response Team (CSIRT). SCU is also responsible for the protection of classified information, as well as ensuring the physical security of eu-LISA premises and staff in three locations: Tallinn, Estonia; Strasbourg, France; and Brussels, Belgium.

SCU comprises four sectors: (1) Security Policy and Coordination Sector (SPCS); (2) Information Security and Assurance Sector (ISAS); (3) Cyber Security Sector (CYBS); (4) Protective Security Sector (PSS)

The Information Security and Assurance Sector (ISAS) is responsible for providing comprehensive information security, business continuity and assurance services to ensure operational resilience and uninterrupted operation of both corporate and JHA information systems/services, as well as the underlying infrastructure hosting the systems.

The Cyber Security Sector (CYBS) is responsible for safeguarding the integrity of eu-LISA's digital assets, in particular EU's JHA information systems, infrastructure and data entrusted to the Agency. The main objective is

¹ Date of publication: 10 February 2025

to ensure the integrity, confidentiality and availability of systems and services to stakeholders in the EU's JHA community.

About the job

Working under the supervision of the Head of Sector and reporting to the Head of the Security Unit, you will support eu-LISA's mandate and ensure that the Agency achieves its objectives, enhances its reputation, and answers stakeholders' needs.

You will be able to apply to one (1) or both profiles (Profile A and Profile B) listed below.

Your tasks will include a wide range of responsibilities that extend beyond the following list:

Profile A: Security Officer - Information Security and Assurance Sector

- Assess information security and continuity risks, threats and business impact and take appropriate action;
- Establish and manage prevention, detection, correction and remediation measures to security and continuity risks;
- Monitor emerging security threats and developments to ensure the effectiveness of information security processes and controls;
- Develop and implement Information Security and Business Continuity strategies and frameworks;
- Implement security techniques within application, processes, networks or systems under the area of responsibility;
- Contribute to shaping the organisation's cybersecurity policies and continuity plans;
- Design and propose a secure and resilient architecture aligned with the organisation's strategy and policies and identify potential gaps;
- Integrate security and privacy principles into on-premises and cloud-based systems by default and by design;
- Conduct a security requirements analysis, including user, business, stakeholder and functional/non-functional aspects;
- Create and maintain architectural documentation, ensuring compliance with cybersecurity standards;
- Foster secure and resilient application development practices throughout the application development lifecycle;
- Provide information security and business continuity training and education to enhance awareness and compliance.

Profile B: Security Officer - Cyber Security

- Deploy, operate and maintain a Security Incident and Event Management solution (SIEM) in an all-cloud solution or on premises environment (e.g Splunk, Sentinel);
- Design, build and optimise systems and processes for automated detection of malicious or unauthorised activities;
- Implement and operate cybersecurity solutions (i.e. Privileged Access Management systems, Public Key Infrastructure solutions, Certificate Lifecycle Management solutions, cybersecurity deception solution and Web Application Firewalls);
- Collect, analyse and evaluate security incident reports; perform and/or coordinate detailed technical analysis of incidents and associated artefacts;

- Implement and manage cloud-based security controls, such as identity management, security monitoring, cloud security posture management, cloud workload protection.

Eligibility criteria

To be eligible for recruitment and selection, you need to meet the following formal criteria, which need to be fulfilled by the deadline for applications:

General conditions

- You produce the appropriate character requirements for the duties involved;
- You are engaged within eu-LISA as Temporary Staff 2(f) in function group AD, grade 5-7, on the closing date for applications and on the day of filling the post;

Selection criteria

eu-LISA aims to establish a reserve list from which to source the best talent. The suitability of candidates will be assessed against the following criteria during different stages of the selection procedure:

Professional experience and knowledge

Profile A: Information Security and Assurance

- Professional experience similar to the duties outlined in the section “About the job” for profile A;
- Knowledge of necessary adjustments to security and business continuity frameworks;
- Ability to draft cybersecurity and business continuity architectural and functional specifications;
- Ability to recommend cybersecurity and resilience architectures tailored to the identified risks, stakeholders’ needs and budget constraints;
- Ability to design and implement secure and resilience on-premises and cloud systems balancing security and business continuity requirements with business objectives.

Profile B: Cyber Security

- Professional experience similar to the duties outlined in the section “About the job” for profile B;
- Ability to develop, implement, maintain, patch, upgrade and test cybersecurity solutions;
- Ability to lead and coordinate incident response actions during cybersecurity incidents;
- Ability to evaluate emerging technologies, trends and the threats landscape;

Personal competencies - Applicable to both profile A and profile B

- Ability to define and communicate requirements and/or policies across various audiences and get their buy-in;
- Ability to develop positive business relationships in a diverse stakeholder environment while displaying understanding of their different contexts and perspectives;
- Ability to apply critical thinking and structured problem-solving approaches to develop effective solutions;
- Ability to stay up to date with industry trends, technologies, and best practices;

- Demonstrate excellent organisational skills, maintain a clear overview of multiple tasks and an ability to prioritise towards deadlines and focus on key objectives;
- Ability to act upon eu-LISA's [values](#) and guiding principles (We get the job done - We take ownership - We are all role models - We act together as one).

Language

- Strong language skills in English, both orally and in writing, at least at the C1² level.

Advantageous

- Relevant security and business continuity certifications;
- Experience in highly available IT infrastructure administration;

Application process and next steps

Ready to join us in building a safer Europe? Apply now!

Before submitting your application, you should carefully check whether you meet all eligibility requirements.

Please complete your application form via the e-recruitment platform [here](#). Due to the fact that this is an internal selection, one must select 'Internal' next to the 'Selection procedure type' field and click 'Search' [here](#).

eu-LISA does not accept applications submitted by any other means (e.g., e-mail or post), or any spontaneous applications. Your application should contain personal details, educational background, professional experience, language proficiency, motivation letter, and responses to pre-screening questions if applicable. Candidates are requested to support their application with adequate, concise examples of their work experience and qualification, especially if not directly addressed in the duties listed in the application under professional experience.

Please note that if at any stage of the selection procedure it is established that any of the requested information provided by a candidate is false, they will be disqualified.

If a candidate reaches the reserve list stage, they will be requested to supply documentary evidence in support of the statements that they made for this application.

If you encounter any difficulties during the application process or have any further questions, please do not hesitate to reach out to the Talent Acquisition Service. Feel free to send an email to eulisa-RECRUITMENT@eulisa.europa.eu.

Join our diverse team, where you will have the opportunity to grow both professionally and personally while enjoying the journey.

² Cf. Language levels of the Common European Framework of reference: <http://europass.cedefop.europa.eu/en/resources/european-language-levels-cefr>

Selection procedure

The selection procedure includes the following steps:

- Candidates are invited to indicate the profile (profile **A** OR/AND profile **B**) they are applying for. Candidates can choose to apply either for one (1) or both profiles depending on their interest and competencies;
- A Selection Committee, designated by the Appointing Authority, is established for the selection procedure;
- Each application is checked to verify whether the candidate meets the eligibility criteria;
- All eligible applications are evaluated by the Selection Committee based on a combination of certain selection criteria defined in the Vacancy Notice;
- The quality of the information provided by the candidate in their application is of utmost importance. Candidates are requested to support their application with adequate, concise examples of their work experience (including traineeships, voluntary work etc), and qualification, especially if not directly addressed in the duties listed in the application under professional experience. Certain selection criteria may be assessed jointly and some criteria may be assessed in two or more stages of the selection procedure;
- Once the list of the most qualified candidates is determined, a preliminary assessment may take place (e.g., a pre-recorded video interview and/or a remote written test)³ prior to the shortlist phase;
- In the shortlist phase⁴ consisting of a shortlist interview which may be complemented by a written test, the Selection Committee scores the candidates in accordance with the selection criteria. Candidates may also be required to prepare a presentation on a topic to be presented during the shortlist phase, which would be evaluated as part of the shortlist interview;
- In order to be included in the reserve list, candidates must receive at least 60% of the maximum scores in the shortlist phase;
- Interviews and written tests are predominantly conducted in English⁵.
- After the shortlist phase, the Selection Committee establishes a non-ranked list of the most qualified candidates to be included in a reserve list and proposes it to the Appointing Authority;
- The Appointing Authority may choose from the reserve list a candidate for the post;
- Candidates included in the reserve list may be engaged for the same or similar post depending on eu-LISA's needs and budgetary situation;
- All shortlisted candidates will be informed whether or not they have been included in the reserve list. Candidates should note that inclusion in a reserve list does not guarantee engagement.

³ The Selection Committee has the discretion to choose between remote and on-site interviews/tests as deemed appropriate. For remote interviews, the Selection Committee reserves the right to conduct the interview using an online video interviewing tool for synchronous and/or asynchronous (e.g., recorded) interviews.

⁴ Same applies as per previous footnote.

⁵ As English is eu-LISA's working language, the selection procedure will be predominantly conducted in English, except when English is the mother tongue of a candidate or when the mother tongue of the candidate is not an official language of the European Union. In these cases, some of the interview and/or written test questions may be asked in the language indicated as their 2nd EU language.

Please note that the Selection Committee's work and deliberations are strictly confidential. Any contact with its members is strictly prohibited.

English is eu-LISA's working language. Any communication related to the selection procedure will be conducted in English.

Assignment and conditions of employment

The selected candidate will be assigned by the Authority Authorised to Conclude Contracts of employment from the final list of suitable candidates. Once the candidate receives an assignment offer, they may be required to accept the offer within a short timeframe and be available to start the contract as agreed with their line manager.

The successful candidate will be assigned to the new post according to the assignment decision without an impact on their current contract (with an amendment to the employment contract).

All selected candidates will need to have, or be in a position to obtain, a valid Personnel Security Clearance Certificate depending on the specific job profile. Failure to obtain the required security clearance certificate from the candidate's National Security Authority, either during or after the expiration of the probationary period, will give eu-LISA the right to terminate any applicable employment contract.

Protection of personal data

eu-LISA ensures that candidates' personal data is processed in accordance with Regulation (EU) No 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 data⁶.

The legal basis for the selection procedure of Temporary Staff (TA 2(f)) are defined in the Conditions of Employment of Other Servants of the European Communities⁷.

The purpose of processing personal data is to enable selection procedures.

The selection procedure is conducted under the responsibility of eu-LISA's Human Resources Unit ('HRU'). The controller, in practice, for personal data protection purposes is the Head of the Human Resources Unit.

The information provided by the candidates will be accessible for a limited number of authorised HRU personnel, to the Selection Committee, and, if necessary, to the Executive Director, Security and/or the Legal personnel of eu-LISA.

⁶ Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018, OJ L 295, 21.11.2018, p. 39.

⁷ CEOS, in particular the provisions governing conditions of engagement in Title II.

Almost all fields in the Application Form are mandatory; the answers provided by the candidates in the fields marked as optional will not be taken into account to assess their merits.

Processing begins on the date of receipt of the application. eu-LISA's data storage policy is as follows:

- for applications received but not selected: the paper dossiers are filed and stored in archives for two (2) years after which time they are destroyed;
- for candidates included in a reserve list but not recruited: data is kept for the period of validity of the reserve list + one (1) year after which time it is destroyed;
- for recruited candidates: data is kept for a period of ten (10) years as of the termination of employment or as of the last pension payment after which time it is destroyed.

All candidates may exercise their right of access to and rectification or erasure of their personal data or restriction of processing.

In the case of identification data, candidates can rectify the data at any time during the procedure. In the case of data related to the admissibility criteria, the right of rectification cannot be exercised after the closing date of applications.

Any substantiated query concerning the processing of the candidate's personal data should be addressed to the eu-LISA's HRU (eulisa-RECRUITMENT@eulisa.europa.eu).

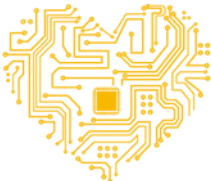
Candidates may have recourse at any time to eu-LISA's Data Protection Officer (dpo@eulisa.europa.eu) and/or the European Data Protection Supervisor (edps@edps.europa.eu).

Appeal procedure

If a candidate considers that they have been adversely affected by a particular decision, they can lodge a complaint under Article 90(2) of the Staff Regulations of Officials of the European Union and Conditions of employment of other servants of the European Union, to the following address:

eu-LISA
(European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice)
Vesilennuki 5
10415 Tallinn, Estonia

The complaint must be lodged within three (3) months. The time limit for initiating this type of procedure starts from the time the candidate is notified of the act adversely affecting them.

THE DIGITAL  **OF SCHENGEN**

