Vacancy for a post of ICT Security Assistant (Temporary Agent, AST 4) in the European Asylum Support Office (EASO)

REF.: EASO/2018/TA/022

Publication	**External**
Title of function	**ICT Security Assistant**

1. WE ARE

The European Asylum Support Office (hereinafter referred to as "EASO"), established by Regulation 439/2010[1], strengthens European Union (EU) Member States' practical cooperation on asylum, enhances the implementation of the Common European Asylum System (CEAS) and supports Member States whose asylum and reception systems are under particular pressure.

Specifically, EASO focuses on three main tasks:

1. Supporting practical cooperation among Member States on asylum mainly through training, quality activities, country of origin information (COI), statistics and analysis, specialized expert networks, practical cooperation workshops, thematic support on unaccompanied minors, trafficking in human beings and gender;

2. Supporting Member States under particular pressure through emergency support, including the deployment of asylum support teams to assist EU Member States in managing asylum applications and in putting in place appropriate reception facilities;

3. Contributing to the implementation of the CEAS by collecting and exchanging information on best practices, drawing up an annual report on the asylum situation in the EU covering the whole asylum procedure in EU Member States and adopting technical documents, on the implementation of the new EU asylum acquis.

The headquarters of EASO are located at the Valletta Harbour (Malta).

2. WE PROPOSE

The overall purpose of the ICT Security Assistant is to support the Agency in the management of the security and business continuity management. He/she will work under the direct supervision of the Head of ICT Unit. The ICT Security Assistant's main duties will entail:

1. Performing the business and security risks assessments as part of the initial deployment process of the new system(s) and of the further developments;

2. Support to the design of the security architecture of the systems and the security requirements for the systems;

[1] Regulation (EU) No 439/2010 of the European Parliament and of the Council of 19 May 2010 (OJ L 132, 25.5.2010, p.11).

3. Drafting the security and resilience requirements for the inclusion in the technical specifications of tender processes, for the initial deployment of the new system(s) and for the further developments;
4. Participating in the technical evaluation of the offers from contractors for the initial deployment of the new system(s) and their further developments,
5. Supporting any other procurement related process concerning the security of the system(s);
6. Supporting the project manager(s) and the project team(s) during the project activities and process regarding security and business continuity areas;
7. Participating in the elaboration of the use-cases and test-cases security related, specific to the technical implementation of the system(s);
8. Implementing and testing the fulfilment of the technical security requirements for the system(s);
9. Monitoring the security logs and configuring the systems in order to identify any possible incident or event security related;
10. Continuously performing security risk assessments, by analysing and assessing the specific threat and vulnerabilities of the system;
11. Performing any internal security audit of the system, as required;
12. Supporting the technical service desk team and any other user of the systems in the process of administrating/using the system(s);
13. Implementing the Security Incident Management System at the system(s) level;
14. Developing system specific security policies, standards, procedures and guidelines regarding the management and use of the system;
15. Reporting, as necessary, to senior management about the security of the systems;
16. Supporting in the technical and procedural implementation of the specific business continuity and disaster recovery controls for the system(s);
17. Periodically performing system penetration tests and other security tests regarding the system(s);
18. Ensuring the correct configuration of security components in different systems, in collaboration with the operational teams;
19. Carrying out any other relevant duties assigned by the Head of ICT Unit.

3. WE LOOK FOR

A) Eligibility criteria

Candidates will be considered eligible for selection on the basis of the following formal criteria to be fulfilled by the deadline for applications:

1. Have a level of post-secondary education attested by a diploma and, after having obtained the diploma, at least 9 years of appropriate professional experience, or

Have a level of education attested by a diploma and giving access to post-secondary education, and after having obtained the diploma, at least 12 years of appropriate professional experience;
2. Be nationals of one of the Member States of the European Union, Lichtenstein, Norway or Switzerland;
3. Be entitled to their full rights as citizens;
4. Have fulfilled any obligations imposed on them by the laws on military service;
5. Possess a thorough knowledge of one of the official EU languages and a satisfactory knowledge of another of these languages to the extent necessary for the performance of the duties pertaining to the post;
6. Meet the character requirements for the duties involved[2];
7. Be physically fit to perform the duties linked to the post[3].

B) Selection criteria

If the eligibility criteria set out in section *A) Eligibility criteria* are met, the candidates' applications will be evaluated on the basis of the selection criteria below. The most suitable candidates will be invited to an interview.

Essential

1. Proven cumulative professional experience of at least 3 (three) years in the area of information security;
2. Professional experience in security monitoring, threat detection and incident response;
3. Professional experience in proactively and iteratively searching through networks and applications to detect and isolate advanced threats that evade existing security solutions (Cyber threat hunting);
4. Professional experience in the methods, techniques and representative solutions in one or more of the following domain areas:
    a. Infrastructure security components, including LAN and wireless network security controls as well as perimeter security controls;
    b. Database security and monitoring;
    c. Internet security controls and best practices;
    d. Application security (OWASP Application Security and Verification);
    e. Security Event and Information Management (SIEM);

Advantageous

1. Professional experience in security assessments, IT security audits,
2. Security testing, vulnerability assessments and penetration testing;
3. Professional experience in cyber security incident investigations (e.g. forensic analysis, malware analysis, log analysis);

[2] Only diplomas issued by EU Member State authorities and diplomas recognized as equivalent by the relevant EU Member State bodies are accepted. If the main studies took place outside the European Union, the candidate's qualification must have been recognized by a body delegated officially for the purpose by one of the European Union Member States (such as a national Ministry of Education) and a document attesting so must be submitted if you have been invited for an interview. This will enable the selection board to assess accurately the level of the qualifications.

[3] Before the appointment, the successful candidate shall be asked to provide an extract from their police file.

[4] Before the appointment, a successful candidate shall be medically examined by one of the institutions' medical officers in order that EASO may be satisfied that he/she fulfils the requirement of article 28(e) of the Staff Regulations of the Officials of the European Communities.

4. Professional experience in the methods, techniques and representative solutions in the following domain areas:
    a. Authentication and authorisation methodologies (including Identity and access management);
    b. Use of encryption technologies (including high assurance crypto solutions);
    c. Security controls in storage solutions design;
    d. Security controls in server and client virtualisation solutions.
5. Professional experience obtained in a multicultural environment, preferably in International institutions or agencies or government agencies;

Characteristics to be assessed during interviewing process

Candidates invited to the interviewing process (interview and written test) will be assessed on the following criteria that are essential to the post:

1. Ability to communicate clearly and to present complex subjects simply, both orally and in writing;
2. Ability to work under pressure and with tight deadlines, to make timely decisions, to reprioritize tasks responding to changes in a rapidly evolving work environment;
3. A high level capacity to organise and plan work accurately and with attention to details, be pro-active and have the ability to handle multiple tasks when required;
4. A supportive and helpful approach to others, with a cooperative and service-oriented attitude, good communication and interpersonal skills and the ability to cooperate smoothly in a multicultural environment.
5. Good drafting and communication skills in English both orally and in writing, at least at level C1;

4. SELECTION AND APPOINTMENT

The Regulation which provides the legal basis for EASO was adopted in May 2010 (Official Journal of the European Union L 132 of 29.5.2010).

Eligibility of candidates will be assessed by a Selection Committee according to compliance with all eligibility criteria by the closing date for the submission of applications.

The applications of the eligible candidates will also be assessed against the selection criteria. Following this assessment, the best ranking candidates may be invited for a written competency test and an interview, which will be held for the most part in English.

The interview will consist of the following components:

- General aptitude and language abilities to the extent necessary for the performance of their duties in accordance with Article 12.2(e) of the Conditions of Employment of other Servants of the European Communities (CEOS);

- Specific competences with reference to the applicants' profiles in line with the selection criteria of the present Vacancy Notice.

Candidates invited to an interview will be required to bring with them originals and copies of the documents listed below:

- A document proving their citizenship (e.g. passport);
- Certificates attesting their educational and professional qualifications, in particular those giving access to the profile in question;
- Documentary evidence of their professional experience after the date on which the candidate obtained the qualification giving access to the profile in question, clearly indicating the starting and finishing dates, whether full or part time, and the nature of the duties carried out.

The Selection Committee will propose a shortlist of successful candidates to the Appointing Authority, who will decide on the appointment of the successful candidate and the establishment of a reserve list for the post advertised. Candidates shall note that inclusion on the reserve list does not guarantee recruitment. Recruitment will be based on availability of posts and budget.

The reserve list for this post will be valid until 31 December 2019 and may be extended at the discretion of the Appointing Authority.

Prior to contract signature, the successful candidate will be asked to undergo a compulsory medical examination by one of the institutions' medical officers in order that EASO may be satisfied that he/she fulfils the requirement of Article 28(e) of the Staff Regulations of the Officials of the European Communities.

5. EQUAL OPPORTUNITIES

EASO applies an equal opportunities policy and accepts applications without distinction on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

6. CONDITIONS OF EMPLOYMENT

The Temporary Agent will be appointed by the Executive Director, upon recommendation of the Selection Committee, following the selection procedure.

He/she will be recruited as a temporary agent pursuant to Article 2(f) of the CEOS for a period of **5 years** which may be renewed. The temporary agent post in question will be placed in group AST 4.
Successful candidates who are recruited will undergo an initial probation period of nine months.

The pay for a **Temporary Agent, AST 4 (step 1)** consists of a **basic salary of 4,160.50 €** weighted by the correction coefficient (for Malta currently 86.5%) supplemented with various allowances, including family allowances. The salaries of staff members are subject to a Community tax deducted at source. Staff members are exempt from national tax on salary and are members of the Community social security and pension schemes.

For further information on working conditions of temporary staff please refer to CEOS: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1962R0031:20140101:EN:PDF

The place of employment is **Valletta Harbour (Malta)**.

7. APPLICATION PROCEDURE

For applications to be valid, candidates shall:

- Use the official application form provided on the EASO website. The application must be completed in English, and all parts must be completed in full.
- Send their application by email to: applications@easo.europa.eu by the deadline.
- The subject of the e-mail should include the reference of this vacancy, followed by the candidate's surname.

Incomplete applications will be disqualified and treated as non-eligible. Candidates who use the same application to apply for more than one post will also be disqualified.

Please note that the selection process may take several months.

In order to facilitate the selection process, all correspondence to candidates concerning this vacancy will be in English.

Under no circumstances should candidates approach the Selection Committee, directly or indirectly, concerning this recruitment. The Appointing Authority reserves the right to disqualify any candidate who disregards this instruction.

Closing date:

The closing date for submission of the applications is **17 January 2019 at 13:00h** (Brussels time). EASO will disregard any application received after this date and time.

Applicants are strongly advised **not to wait until the last day** to submit their applications, since heavy internet traffic or a fault with the internet connection could lead to difficulties in submission. The EASO cannot be held responsible for any delay due to such difficulties.

If at any stage in the procedure it is established that any of the information provided by a candidate is incorrect, the candidate in question will be disqualified.

8. DATA PROTECTION

The purpose of processing of the data submitted by the candidate is to manage the application(s) of the candidate in view of a possible selection and recruitment at EASO.

EASO does not make public the names of successful candidates on reserve lists. However, it is possible that, for the purposes of recruitment and related planning purposes, members of the EASO management team may have access to reserve lists and, in specific cases, to the application form of a candidate (without supporting documents, which are kept in confidence by the personnel department). Application files of non-recruited candidates are kept for two years from the expiry date of the reserve list after which time they are destroyed.

The personal information requested will be processed in line with Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data.

9. APPEAL PROCEDURES

Pursuant to Article 90(2) of the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the Union, a candidate may submit a complaint against an act affecting him/her adversely. The complaint must be lodged within 3 months from the date of notification to the following address:

The Executive Director
European Asylum Support Office
MTC Block A, Winemakers Wharf, Grand Harbour Valletta, MRS 1917
Malta

Should the complaint be rejected, pursuant to Article 270 of the Treaty on the Functioning of the European Union and Article 91 of the Staff Regulations of Officials and the Conditions of Employment of Other Servants, a candidate may request judicial review of the act. The appeal must be lodged within 3 months from the date of notification to the following address:

European Union Civil Service Tribunal
Boulevard Konrad Adenauer
L-2925 Luxembourg
Luxembourg

Any citizen of the European Union or any natural or legal person residing in a Member State may make a complaint for maladministration pursuant to Article 228(1) of the Treaty on the Functioning of the European Union. The complaint must be lodged within two years of becoming aware of the facts on which the complaint is based to the following address:

European Ombudsman
1, Avenue du President Robert Schuman -BP 403
F-67001 Strasbourg Cedex
France

Please note that complaints to the European Ombudsman do not have the effect of suspending the period mentioned in Articles 90 and 91 of the Staff Regulations of Officials and the Conditions of Employment of Other Servants for lodging complaints or submitting an appeal pursuant to Article 270 of the Treaty on the Functioning of the European Union.