FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

VACANCY NOTICE – TEMPORARY STAFF

Reference number: RCT-2017-00043

Senior ICT Security Officer (Team Leader)

Post (business title):	**Senior ICT Security Officer (Team Leader) – 1 post**
Sector/Unit/Division:	ICT Security Team / ICT Unit / Corporate Governance
Function group / Grade / Post title:	Temporary Staff, AD8, Principal Administrator
Location:	Warsaw, Poland
Starting date:	June 2018 (desired)
Level of Security Clearance:	SECRET UE / EU SECRET
Closing date for applications	(MIDDAY) 13 March 2018 at 12:00 h[1]

1. BACKGROUND

The European Border and Coast Guard Agency (Frontex) has been established under Regulation (EU) 2016/1624 of 14 September 2016. The agency was created on the foundations of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (established under Council Regulation (EC) No 2007/2004), which has been coordinating operational activities at the EU external border since 2005.

Frontex is located in Warsaw, Poland and is in the process of significantly increasing the size of its staff from the current number of more than 530 to meet its expanded tasks.

The agency's key tasks include:

- Operational and technical assistance to the EU member states at their external borders by coordinating joint border control operations including deployment of vessels, aircraft and other equipment and border and coast guards from EU countries;
- Coordination of border surveillance and law enforcement activities being part of maritime security in cooperation with national authorities and EU agencies such as Europol, EMSA and EFCA;
- Situation monitoring of EU's external borders and risk analysis of all aspects of border and coast guard management, including assessment of the EU Member State's border control authorities ability to face migratory pressure and different challenges at their external borders;
- Assisting member states in returning nationals of non-EU countries who do not have the right to remain on the territory of the EU;
- Development of training programmes for European border and coast guards;
- Monitoring new technological developments in the field of border control and acting as an interface between research institutions, industry and national border and coast guard authorities;
- Cooperation with EU and international organisations in the area of border and coast guard management, security, and prevention of cross-border crime (including terrorism);

[1] *Date of publication: 12 February 2018.*

- Assist non-EU countries in the context of technical and operational cooperation on border management including return of non-EU nationals, in the framework of the EU external relations policy.

For more information, please refer to our website: http://www.frontex.europa.eu.

2. THE CORPORATE GOVERNANCE AND THE ICT UNIT

The general mission of Corporate Governance is to give all necessary support and assistance to operational units and other units and entities of the Agency to allow them to function in the smoothest possible way. Corporate Governance functions include Budget, Financial and Corporate Services Unit, Legal and Procurement Unit, Human Resources and Security Unit, and Information and Communication Technology Unit.

Frontex ICT Unit is responsible to maintain, support and further develop ICT infrastructure, IT services and specific IT solutions put in place for the various business divisions and units in Frontex. It is also responsible for maintaining all the systems at an adequate level of security and to constantly improve the security solutions as new threats appear.

Within the ICT Unit, the ICT security team is responsible for the matters related to ICT security such as drafting of policies and procedures, information for users, delivery of security related requirements for modification of existing system, input of requirements for architecture and design purposes of new IT solutions, review of systems, architectures and design, monitoring and investigation of IT security related incidents, performance of risk and privacy analysis of systems or processes, performance or supervision of IT security tests, coordination and follow up of implementation of recommendations and corrective measures following such tests and internal check of compliance of systems to defined rules and policies.

3. DUTIES AND RESPONSIBILITIES LINKED TO THE POST

The Senior ICT Security Officer (Team Leader) will play a crucial role in the management and the awareness of security of Frontex IT systems and data as well as in the development, the communication and the enforcement of the IT security principles, policies and procedures and in the support of the different units in the development of adequate security requirements of business systems.

The Senior ICT Security Officer (Team Leader) will be managing ICT security team, advising the Head of ICT Unit about all ICT security issues and developing sound ICT security related policies and procedures applicable to IT operations as well as on the use of IT equipment.

Reporting to the Head of Unit, the main duties related to this post are:

- To redefine an ICT systems security program, including budget and resource requirements;
- To draft and propose ICT security policies in line with the ICT Strategy, the nature and characteristics of the information processed by IT systems and the scope and purpose of the systems;
- To participate in system specification and development processes in order to define and enforce security requirements and improvements;
- To ensure correct configuration of security components in different systems, together with the Information System and Network Administrators;
- To liaise with the Frontex Security Sector concerning all ICT relevant security matters;
- To organize and coordinate execution of security tests, to analyse the results of IT security tests and associated recommendations, to establish corrective plans at the level of ICT Unit, to follow up the implementation of countermeasures;
- To prepare terms of reference and procurement requests in the area of competence for required goods and services;
- To advise the Head of Unit on ICT security matters;

- To maintain appropriate contacts with special interest groups, other agencies, CERT-EU, forums or professional associations in the field of ICT systems security.

4. QUALIFICATIONS AND EXPERIENCE REQUIRED

4.1. Eligibility criteria

To be eligible, an applicant shall:

- Possess a level of education which corresponds to **completed university studies** attested by a diploma when the normal period of university education is **four years or more** (of full-time education);

or

- Possess a level of education which corresponds to completed university studies attested by a diploma **followed by at least one year full-time professional experience**, when the normal period of university education is **at least three years** (of full-time education);

- In addition to the above, by the closing date for applications, possess at least **9 years** of proven full-time professional experience after the diploma was awarded;

  Only qualifications that have been awarded in EU Member States or that are subject to the equivalence certificates issued by the authorities in EU Member States shall be taken into consideration.

  Professional experience will be taken into account after the award of the minimum qualification certifying the completion of the level of studies required above in the first two bullet points. Only duly documented professional activity is taken into account.

  Only the required education will be taken into account.

  ANY GIVEN PERIOD MAY BE COUNTED ONLY ONCE (in order to be calculated as eligible, years of studies or professional experience to be taken into account shall not overlap with other periods of studies or professional experience, e.g. if the applicant had a full-time job and did freelance consultancy work in the evenings and weekends, the days spent on the latter will not be added to the period).In case of part-time work the professional experience will be calculated pro-rata in line with the workload stated by the applicant. Compulsory military service or equivalent civilian service accomplished after achieving the minimum qualification stated in the first two bullet points shall be taken into consideration as professional experience if the official documentation is provided.

- Produce evidence of thorough knowledge of one of the languages of the European Union and of satisfactory knowledge of another language of the European Union to the extent necessary for the performance of his/her duties;
- Be a citizen of one of the Member States of the European Union or the Schengen Associated Countries and enjoy full rights as its citizen;
- Have fulfilled any obligations imposed on them by the laws of the country of citizenship concerning military service.

Additionally, in order to be engaged, the appointed applicant shall:

- Produce the appropriate character references as to his suitability for the performance of his duties (a criminal record certificate or equivalent certificate, not older than six months) and a declaration in relation to interests that might be considered prejudicial to his/her independence;
- Be physically fit to perform their duties[2].

[2] *Before the engagement, the successful applicant shall be medically examined by the EU medical service to fulfil the requirement of Article 13 of Conditions of Employment of Other Servants of the European Communities (OJ L 56, 4.3.1968, p. 10), as lastly amended.*

4.2. Selection criteria

Suitability of applicants will be assessed against the following criteria in different steps of the selection procedure. Certain criteria will be assessed only for shortlisted applicants during interviews (and or tests):

4.2.1. Professional competences

1. University degree or post-graduate degree in information technology or information management;
2. Experience in leading a team (preferably including managing staff, appraisal, holidays, missions) and financial resources for at least two years;
3. Good knowledge of ISO 27000 family standards;
4. Detailed knowledge of system security vulnerabilities, threats and exploit mechanisms, penetration testing, remediation techniques and risk analysis methodology;
5. Experience in developing and implementing ICT security operation capabilities, configuration of anti-malware solution and good understanding of encryption mechanisms;
6. Good knowledge of Security features and configuration from Microsoft PCs (Windows 7 or windows 10), Servers (AD, ADFS, file servers, exchange, PKI, Security Compliance Manager, Group Policy);

Besides, the following attributes would be considered advantageous

7. Experience in mobile device security;
8. Having practical experience of the accreditation process in EU institutions;
9. Good knowledge of security features and of configuration for UBUNTU servers and OpenLDAP and experience in the setup and management of a SIEM systems;
10. Being holder of a relevant certification in the area of ICT security (CISSP, CISM, CISA, etc.) as well as of the Personal Security Certificate equivalent to Secret UE / EU Secret.

4.2.2. Personal qualities and competences

11. Very good communication skills in English, both orally and in writing (using Microsoft Office applications) and excellent interpersonal skills; an ability to develop and maintain effective working relationships with a wide range of internal and external stakeholders and an ability to understand organisational dynamics;
12. Capability to organize, coordinate and manage work and responsibilities and deliver expected results including an ability to work effectively both independently and within a multicultural team and an ability to cope with work pressure in a dynamic and changing working environment;
13. Professional and ethical behaviour, strong sense of initiative, responsibility, commitment and customer oriented work ethic;
14. Ability to independently execute ICT projects through the complete project lifecycle.

5. INDEPENDENCE AND DECLARATION OF INTEREST

The selected applicant(s) will be required to make a declaration of commitment to act independently in Frontex' interest and to make a declaration in relation to interests that might be considered prejudicial to his/her independence.

6. EQUAL OPPORTUNITIES

Frontex applies an equal opportunities policy and accepts applications without distinction on grounds of age, race, political, philosophical or religious conviction, sex or sexual orientation and regardless of disabilities, marital status or family situation.

7. SELECTION PROCEDURE

The selection procedure includes the following steps:

- After registration, each application is checked in order to verify whether it meets the eligibility criteria;

- All the eligible applications are evaluated by an appointed Selection Committee based on a combination of certain selection criteria defined in the vacancy notice (some criteria will be assessed only for shortlisted applicants during interviews and/or tests). Certain selection criteria may be assessed jointly and some criteria may be assessed in two or more steps of the selection procedure;
- Best-qualified applicants, who obtain the highest number of points within the application evaluation and who are matching the best the evaluated selection criteria, will be shortlisted and invited for a competency test and an interview; the names of the Selection Committee members will be disclosed to the applicants invited for the interview;
- The interview will be held in English;
- During the interview, the Selection Committee will examine the profiles of applicants and assess their relevancy for the post in question. Certain selection criteria may be assessed jointly and some criteria may be assessed in two or more steps of the selection procedure. In order to support the evaluation via interview, shortlisted applicants may be required to undergo written competency tests and complete part of the process in their second language;
- Applicants invited to the interview/test will be requested to present, on the day of the interview, originals of their diploma(s) and evidence of their professional experience, clearly indicating the starting, finishing dates and workload;
- As a result of the interviews, the Selection Committee will recommend the most suitable applicant(s) for the post in question to the Executive Director of Frontex. An additional interview with the Executive Director and/or the Deputy Executive Director or other relevant manager may be arranged before the final appointment. Non-recruited and suitable applicants will be proposed for a reserve list, which may also be used to fill similar vacant post depending on the needs of Frontex. This reserve list will be valid for 2 years (the validity period may be extended). Each interviewed applicant will be notified in written whether or not he/she has been placed on the reserve list. Applicants should note that the placement on the reserve list does not guarantee an employment offer.

The work and deliberations of the Selection Committee are strictly confidential and any contact of an applicant with its members is strictly forbidden.

8. APPOINTMENT AND CONDITIONS OF EMPLOYMENT

The most successful applicant will be appointed by the Executive Director of Frontex.

The successful applicant will be engaged as temporary staff pursuant to Article 2(f) of the Conditions of Employment of Other Servants of the European Communities (CEOS). The temporary post in question is placed in the following function group and grade: **AD8**.

The staff member's remuneration consists of a basic salary and allowances. The staff member may be entitled to various allowances, in particular to an expatriation (16 % of basic gross salary) or to a foreign residence allowance (4 % of basic gross salary) – depending on particular situation, and to family allowances (depending on personal situation) such as household allowance, dependent child allowance, pre-school allowance, education allowance.

The remuneration is expressed in EUR, after the compulsory deductions set out in the Staff Regulations or in any implementing regulations is weighted by the correction coefficient for Poland (currently 70.6 %). It can be paid either in EUR or in PLN according to a fixed exchange rate (currently 4.2489 PLN/EUR).

The remuneration of the staff members, the correction coefficient and the exchange rate are updated annually before the end of each year, with retroactive effect from 1 July, in accordance with Annex XI of the Staff Regulations.

The final net calculation (amount payable) is as follows:

Function group, grade and step	**AD8 Step 1**	**AD8 Step 2**
Basic net salary (without any allowances)	3 641 EUR 15 469 PLN	3 769 EUR 16 013 PLN

Household allowances (net)	227 EUR 963 PLN	231 EUR 980 PLN
Expatriation allowances (depending on family situation) (net)	770 – 943 EUR 3 272 – 4 007 PLN	803 – 976 EUR 3 410 – 4 147 PLN
Dependent child allowances for each child (net)	285 EUR 1 210 PLN	285 EUR 1 210 PLN
Preschool allowance (net)	70 EUR 296 PLN	70 EUR 296 PLN
Education allowance (net) up to	386 EUR 1 641 PLN	386 EUR 1 641 PLN

Staff pays an EU tax at source and deductions are also made for medical insurance, pension and unemployment insurance. Salaries are exempt from national taxes. The rate of the solidarity levy is 6 %.

The headquarters agreement with the Polish authorities is effective as of 1 November 2017. Under this agreement the Polish authorities will provide the following main benefits to Frontex expatriate staff:

(a) a reimbursement of tuition cost of each dependent child (as from the age of 2.5 years) attending a school (up to and including secondary school) on Polish territory up to a limit of 35 000 PLN per school year;

(b) limited 12 months' period of reimbursement of VAT on purchases of main household effects to assist a newcomer to settle in Warsaw;

(c) a reimbursement of VAT on a purchase of a private car (this entitlement is renewable after 36 months).

Additionally, this agreement foresees that (an accredited) European School will be set-up in Warsaw in the future to allow dependent children of all Frontex staff (including Polish nationals) to attend a (tuition-free) European-type multilingual education.

Staff is entitled to annual leave of two working days per each complete calendar month of service. On top of that, staff is entitled to a number of additional days of leave depending on the grade, age and distance from the place of origin. In addition, there are on average 18 public holidays per year. Special leave is granted for certain circumstances such as marriage, birth or adoption of a child, etc.

Frontex being a knowledge based organization acknowledges the importance of training provided to its staff. Frontex provides general and technical nature training as well as professional development opportunities that are discussed annually during the staff performance appraisal.

Throughout the period of service staff is a member of the EU pension scheme. The pension is granted after completing a minimum of 10 years' service and after reaching the pensionable age of 66 years. The pensionable age for staff recruited before 1 January 2014 varies between 60 and 65 years. Pension rights acquired in one or more national schemes before starting to work at Frontex may be transferred into the EU pension system.

Staff is covered 24/7 and worldwide by the Joint Sickness Insurance Scheme (JSIS). Staff is insured against sickness, the risk of occupational disease and accident as well as entitled under certain conditions to a monthly unemployment allowance, the right to receive payment of invalidity allowance and travel insurance.

For further information on working conditions please refer to the Staff Regulations and the CEOS.

A contract of employment will be offered for a period of five years, with a probationary period of nine months. The contract may be renewed.

Frontex requires selected applicants to sensitive posts to undergo a security screening procedure and obtain a positive national opinion or respective personal security clearance. The level of the latter depends on the specific post. For this post, the required level of clearance is **SECRET UE / EU SECRET.** Applicants who currently hold a valid security clearance at the above-mentioned level (or higher) may not need to obtain a new one, pending confirmation from their respective National Security Authority. They shall provide Frontex with a security clearance certificate specifying the issuing authority, level and date of expiry. In case the validity of the security clearance expires within six months, a renewal procedure shall be initiated

expeditiously. In case selected applicants do not currently hold a valid and positive security clearance at the above-mentioned level, Frontex will request such from the National Security Authority of the applicants' state of citizenship. In case of a failure to obtain the required security clearance certificate or if the National Security Agency issues a negative opinion at the above-mentioned level after the signature of the contract of employment Frontex has the right to terminate the contract of employment.

9. PROTECTION OF PERSONAL DATA

Frontex ensures that applicants' personal data are processed in accordance with Regulation (EC) No 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 European Union institutions and bodies and on the free movement of such data (12.1.2001, OJ, L 8). Please note that Frontex will not return applications to applicants. This applies in particular to the confidentiality and security of such data.

The legal basis for the selection procedures of temporary staff are defined in the CEOS[3].

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

The selection procedure is conducted under the responsibility of the Human Resources Sector of the Human Resources and Security Unit, within the Corporate Governance of Frontex (HR Sector). The controller for personal data protection purposes is the Head of HR Sector.

The information provided by applicants will be accessible to strictly limited number of staff in Human Resources, to the Selection Committee members and to Frontex management. If necessary it will be provided to the staff of Legal and Procurement Unit or to respective experts in ICT (in case of technical issues with the application).

Processing begins on the date of receipt of the application. Data storage policy is as follows:

- For applications received from not-selected applicants: the data are filed and stored in archives for **2 years and** after this time the data are destroyed;
- For applicants placed on a reserve list but not recruited: the data are kept for the period of validity of **the reserve list + 1 year and** after this time the data are destroyed;
- For recruited applicants: the data are kept for a period of **10 years** after the termination of employment or as of the last pension payment **and** after this time the data are destroyed.

All applicants may exercise their right of access to and right to rectify personal data. In case of identification data, applicants can rectify those data at any time during the procedure. In the case of data related to the eligibility or selection criteria, the right of rectification can only be exercised by submitting/uploading a new application and it cannot be exercised after the closing date for submission of applications.

Should an applicant have any query concerning the processing of his/her personal data and has substantiated request, he/she shall address them to the HR Sector at jobs@frontex.europa.eu.

Applicants may have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).

10. APPEAL PROCEDURE

If an applicant considers that he/she has been adversely affected by a particular decision he/she can lodge a complaint under Article 90(2) of the Staff Regulations at the following address:

Frontex
Human Resources Sector
Plac Europejski 6
00-844 Warsaw
Poland

[3] *In particular the provisions governing conditions of engagement in Title II, Chapter 3.*

The complaint must be lodged within 3 months. The time limit for initiating this type of procedure starts to run from the time the selection procedure for this post is declared as closed on the Frontex webpage (http://www.frontex.europa.eu).

Applicants also have a possibility to complain to the European Ombudsman. Please note that complaints made to the European Ombudsman have no effect on the time period laid down in Article 91 of the Staff Regulations. Note also, that under Article 2(4) of the general conditions governing the performance of the Ombudsman's duties, any complaint lodged with the Ombudsman must be preceded by the appropriate administrative approaches to the institutions and bodies concerned.

11. APPLICATION PROCEDURE

Note: The way to submit the digital application form to Frontex has recently changed. It is now required to upload the digital application form saved in its original electronic dynamic PDF format (not scanned). Do not use any e-mail communication to submit your application (unless explicitly authorized in writing by Frontex Recruitment team) – such an application will be **automatically disregarded and will not be recorded and further processed.**

Frontex Application Form is to be downloaded (as a dynamic PDF form) from Frontex website under the link provided next to the Reference Number of the post/position. This digital application form is specifically created only for this selection procedure (and shall not be reused for another procedure).

The Frontex Application Form must be:

- Opened in a PDF reader in a MS Windows equipped computer – the recommended version of the PDF reader is the Adobe Acrobat Reader DC *(version 2017.009.20044. You may download this free version here: https://get.adobe.com/uk/reader/).*
- The form is digitally signed and protected against any manipulation or changes. Therefore, applicants shall not try to manipulate and/or alter it – in such a case the digital signature will disappear and the application form will become invalid for subsequent processing resulting in an automatic rejection of such a submission.
- Completed in English. Fields, where you may enter your input, are highlighted in light blue colour. Fields marked with an asterisk (*) indicate a required input. You should be concise, the space for your input is limited by the size of the text boxes.
- Saved and named as follows: 'SURNAME_RCT-2017-00043'.
- After saving, it **shall be submitted to Frontex by uploading it to this URL link**:

  https://microsite.frontex.europa.eu/en/recruitments/RCT-2017-00043

- In case you have technical issues with filling/saving/uploading your electronic application form, you may write to us (in advance of the closing date for submission of applications) at jobs@frontex.europa.eu.
- In case you will submit more than one application in this procedure, Frontex will only assess the latest one and will automatically disregard all your previous applications.

If at any stage of the selection procedure it is established that any of the requested information provided by an applicant is false or misleading, the applicant in question will be disqualified.

Applicants shortlisted for an interview will be requested to supply documentary evidence in support of the statements made in the application. Do not, however, attach any supporting or supplementary documentation with your application until you have been asked to do so by Frontex.

Incomplete applications, applications uploaded after the deadline, sent by an e-mail or applications using inappropriate or altered/manipulated application form will be automatically disregarded by the system and will not be further processed.

Due to the large volume of applications, Frontex regrets that only applicants invited for the interview will be notified on the outcomes. The status of the recruitment procedure is to be found on Frontex website.

Due to high volume of selection procedures handled by Frontex the period between the closing date for applications submission and the end of the shortlisting of applicants for an interview may take more than two months.

The closing date (and time) for the submission of applications is provided on the title page of the Vacancy Notice.

Please keep a copy of the automatically generated submission code that proves that you have submitted/uploaded you application to Frontex.

Applicants are strongly recommended not to wait until the last day to submit their applications.

Frontex cannot be held responsible for any last-minute malfunction due to an overload of the system or for other technical issues applicants may eventually encounter in the very last moment before the deadline.