

JOB DESCRIPTION

Name of the Post: Second Officer in the ICT Infrastructure and Operations Unit with the Information Management and Technology Department (IMT1) – ICT Security

**Reporting to: First Officer ICT Security, Infrastructure and Operations Unit
Head of the Infrastructure and Operations Unit**

1. Purpose of the post

Participate to the maintenance, support and evolution activities of Europol's ICT Security infrastructure. In collaboration with the other IMT Units and groups, provide ICT solutions to business needs.

2. Tasks and Responsibilities

Under the supervision of a First Officer, the post holder will be carrying out the following main duties:

- As part of the ICT Security team, ensure the continued provision of adequate protection in relation to the Europol Computer Systems;
- Perform regular monitoring and analysis of technical logs, including operating system, infrastructure and communications equipment;
- Participate in the design, build, operation and daily verification of the security infrastructure elements including antivirus, audit, VPN, firewall, IDS/IPS and PKI;
- Ensure the provision of procedures, guidelines and policy documents related to security;
- Study, implementation, coordination and documentation of ICT security projects and procedures,
- Advise on ICT security impact assessments including the provision of technical security recommendations in the form of written and verbal reports to in-house projects and activities;

- Provide 3rd line support for incidents and problems related to ICT security;
- Carry out routine tasks such as maintenance, upgrades, updates and providing reports or statistics;
- Stay abreast of recent developments in the ICT security field.

3. Requirements

3.1 General requirements (Art. 24 of the Europol Staff Regulations)

The post holder should:

- **Be a national of one of the Member States of the European Union and enjoy full rights as a citizen;**
- **Have an excellent oral and written command of at least two official languages of the European Union, including English;**
- **Have fulfilled any obligations imposed on him/her by the laws concerning military services;**
- **Produce appropriate character references as to the suitability for the performance of the duties;**
- **Be physically fit to perform the duties;**
- 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, preferably in the area of Information Technology

OR

- Possess a level of education which corresponds to completed university studies attested by a diploma, preferably in the area of Information Technology and appropriate professional experience of at least one year when the normal period of university education is at least three years;
- In addition to the above have at least 6 years of relevant professional work experience in the area of ICT security gained following the award of the diploma..

3.2 Specific skills and competencies required for the post:

The post holder should have:

a. Professional experience:

Essential:

- Experience in the area of web portal and applications security including web server hardening, identity management and application integration;
- Experience in the field of database security (protection and auditing).

Desirable:

- Experience in the field of Microsoft technologies security – including securing systems based on .NET and SharePoint technologies;
- Experience in the area of Microsoft environment security including securing Active Directory, hardening servers, programs and services;
- Experience in the area of configuration, support and maintenance including Firewall, VPN & anti virus solutions.

b. Professional knowledge:

Essential:

Sound knowledge of Information Security principles, including but not limited to:

- Risk analysis methodologies and information security standards;
- Common information security safeguards;
- Significant expertise working with a wide range of IT Security products, vendors and technologies.

Desirable:

- IBM WebSphere environments security;
- Intrusion detection & incident monitoring including knowledge of typical attack patterns and signatures as well as well-known DOS, exploits and vulnerabilities;

c. Technical skills and competencies:

The post holder should:

Essential:

- Be proficient the area of PKI and/or Certificates management and life cycle (SSL, PKI for VPN based systems, user and system based...);

- Have excellent organisational skills including the ability to work under pressure;
- Possess excellent analytical skills.

d. Social skills and competencies:

Essential:

- Possess a high level of interpersonal skills with the ability to work well within a team;
- Possess excellent oral and written communication skills including the ability to communicate technical matters to a non-technical audience;
- Have a high sense of responsibility and integrity, and display initiative and commitment;
- Be capable of working effectively in an international, multi-professional work environment;
- Be willing to work flexible hours at short notice and to participate in an on-call duty roster.

4. Salary

Scale: 7

The basic salary is EUR 4 863, 32.

(Tax deductions and social contributions within Europol amount to approximately 15-20 %)

In addition, when relevant, family allowances can be granted:

- 5% of the basic salary – household allowance;
- EUR 289.03 (net) - per dependant child;
- EUR 628.33 (net) – expatriation allowance

Additional benefits (annual trip home, education allowance, rent and other allowances, excellent health insurance, etc.)

5. Additional Information

5.1 Main dates:

Deadline for application: 11. August 2009
Recruitment procedure: 26. – 27. August 2009
Starting date of employment: as soon as possible but no later than
1 December 2009

5.2 Contact Details:

Should you have further questions on the details of the above position, or should you require any guidance on completing the application form please consult the EUROPOL RECRUITMENT GUIDELINES on www.europol.europa.eu or call +31 (0) 70 302 5298 or +31 (0) 70 353 1628.
