VACANCY NOTICE V/AD/ICT/1/2025

The **European University Institute (EUI),** based in **Florence**, **Italy**
is organising a selection procedure based on qualifications and tests
to draw up a reserve list[1] for the post of

Cyber Incident Responder
in the Information and Communication Technology Service
(Temporary agent post, type 2a, AST04[2])

The European University Institute (EUI) seeks an outstanding and highly motivated individual to safeguard the Institute's cybersecurity posture, lead incident response during attacks, and ensure the effectiveness of security tools and controls.

Who We Are

The **European University Institute (EUI)** at a glance:

- **an international organisation** set up in 1972;
- a research university focusing exclusively on **post-graduate, doctoral and post-doctoral studies,** and **advanced research**;
- located in the hills overlooking the city of Florence, Italy.

The Institute also hosts the Historical Archives of the European Union.

More on our Institution: https://www.eui.eu/About

Our Unit

The **Information and Communication Technology Service (ICT)** provides, among others, digital services, technologies and tools to support the work and activities of the EUI. It is committed to delivering quality customer service and digital solutions to the academic and administrative areas of the EUI community.
The ICT Service provides digital services and support to ensure that all EUI users have access to information via a system that is reliable, fast, campus-wide and fully integrated with the external information world; ensures that EUI staff and researchers are able to maximise their use of the available digital tools; and develops and implements the digital resources required (tools, services, infrastructure, staff, & services) to achieve the strategic goals and objectives of the EUI.

[1] The reserve list may be used to fill similar vacant future positions in other units of the European University Institute. Cf. President's decision No 15/2021of 27 April 2021 laying down a procedure for the use of reserve lists.
[2] Cf. Annex II

Your Key Responsibilities

The EUI is looking for a **Cyber Incident Responder** who will be responsible for monitoring the Institute's cybersecurity posture, managing incidents during cyber-attacks, and ensuring the ongoing functionality of security monitoring tools and security controls. The staff member's key responsibilities include analysing, evaluating, and mitigating the impact of cybersecurity incidents and identifying their root causes and the actors involved. By implementing the Institute's Incident Response Plan, the Cyber Incident Responder restores system functionalities to operational status while collecting evidence and documenting the actions taken. The deliverables of this role include the Incident Response Plan and the Cyber Incident Report. The staff member will be expected to maintaining business continuity in the event of the absence of the Information Security Officer.

The main duties may include the following:

Level of Expertise

- Acting as subject matter expert in incident handling, with hands-on experience in security monitoring and security tools used in on-premises infrastructure and Microsoft and/or Amazon Web Services cloud providers, including:
    - identifying, analysing, mitigating and communicating cybersecurity incidents;
    - assessing and managing technical vulnerabilities;
    - measuring cybersecurity incidents detection and response effectiveness;
    - evaluating the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident;
    - adopting and developing incident handling testing techniques.

Role in administrative processes

- Establishing and updating the incident response procedures;
- Reporting on information security incidents and documenting incident results from analysis and incident handling actions;
- Providing contributions to the Institute's risk register, communicating cybersecurity risks;
- Collecting, analysing and correlating cyber threat information originated from multiple sources;
- Managing and analysing security log files;
- Stand-by duty for incident response needs (cyber-attacks).

Level of autonomy and accountability

- Reporting directly to the Information Security Officer;
- Possessing a high level of autonomy in the implementation of assigned tasks; accountable for own work.

Representation/Communication

- Representing the Information Security Team internally and externally in daily interactions with external Secure Operation Centres (SOCs) and third parties for incident analysis;
- Cooperating with key personnel to report security incidents according to the applicable legal framework.

Policy/Strategy Making

- Contributing to the drafting of documents, analysis and briefings to improve the procedures for incident results analysis and incident handling reporting;
- Contributing to the drafting and updating of information security policies, incident response plan and business continuity documents.

Finance and procurement responsibility

- Drafting contracts and project agreement, preparing calls for tenders in information security;
- Drafting proposals for the provisioning of security services and tools.

Budget management

- Providing contributions to budget estimates for the cybersecurity area at the EUI;
- Contributing by providing insights, such as draft documents or data for the security projects portfolio and annual reports.

Managing people/Role in HR processes

- Supervising the work of external consultants;
- Providing training for IT staff members and user support staff;
- Acting as a coach for junior colleagues.

Your Key Competencies

All staff at the EUI share the following competencies:

- Ethics and integrity
- Working in a multicultural environment
- Accountability
- Delivering quality and results

Competencies specific to **role** include the following:

- Communication skills
- Problem-solving
- Confidentiality
- Ethics & Integrity
- Change management
- Project and Task management

The competencies mentioned above may be assessed at the written test and/or interview stage.

Read more on EUI Competency Framework

What We Offer

- A role in an inspiring community of young scholars with an exclusive focus on master, doctoral and post-doctoral studies;
- A truly multicultural community of 1100 academics at all career stages and administrative staff of approximately 85 different nationalities;
- The commitment to a genuine culture of equality, diversity and inclusion, and to attracting, encouraging and retaining a diverse and highly qualified workforce;
- A world-class research library, the Historical Archives of the European Union, and many other excellent research facilities;
- Language courses and soft skills training opportunities;
- Access to all EUI facilities: library, crèche, cafeteria, gym, participation in seminars and workshops;
- Competitive salary package including health and pension plan;
- A healthy work-life balance in a family-friendly environment.

Read more on Work and Life of EUI Support Staff.

How To Apply

Applications must be submitted electronically using the **online application form** available at https://www.eui.eu/About/JobOpportunities/Open-competitions-for-administrative-posts

CLOSING DATE FOR APPLICATIONS: 30 October 2025 at 23:59 CET

As the EUI is committed to promoting **diversity** and **gender equality** at all levels and in all units in meaningful and lasting ways, we wish to particularly encourage women to apply for this position.

Before completing the online application form you are invited to read ANNEXES I & II that represent an integral part of this vacancy notice.

Annex I – Eligibility and Selection Criteria

ELIGIBILITY CRITERIA

On the closing date for online applications, you must fulfil <u>all</u> the following general and specific conditions:

1. General conditions

- Being a national of a Member State of the European Union;
- Enjoying full rights as a citizen attested by a recent extract from judicial records and/or certificate of good conduct proving no previous conviction for a criminal or administrative offence that could call into question their suitability for performing the duties of the post;
- Having fulfilled any obligations imposed by the laws on military service;
- Being physically fit to perform the duties[3].

2. Specific conditions

2.1 Education (Qualifications)

- A level of post-secondary education attested by a diploma, or
- A level of secondary education attested by a diploma giving access to higher education, and appropriate professional experience of at least three years. This professional experience will be considered part of the educational qualification and will not be taken into account in the required numbers of professional experience under 2.3.

Only diplomas and certificates that have been awarded in EU Member States, or that are the subject of equivalence certificates issued by authorities in the Member States by the deadline for applications, shall be taken into consideration. If your diploma was issued outside the EU, please indicate in your application that you hold an equivalence certificate (*'statement of comparability'*); otherwise, your application will be deemed ineligible.[4]

2.2. Knowledge of Languages[5]

- Main language: have a thorough knowledge of one official language of the European Union; and
- Second language: a satisfactory knowledge of another official language of the European Union to the extent necessary for the performance of the duties.

[3] As a condition for the engagement, the successful candidate shall be medically examined in order for the EUI to prove that they fulfil the requirement of Article 12(2)(d) of the Conditions of Employment of Other Servants

[4] If you have a diploma recognised in an EU Member State, you don't need NARIC recognition for your lower level diploma(s). Example: If you have a Bachelor's degree from a university outside the EU, and a Master's degree from an EU university, you don't need NARIC recognition for the Bachelor's degree. Qualifications/diplomas awarded until 31/12/2020 in the United Kingdom are accepted without further recognition. For diplomas awarded after this date (from 01/01/2021), a NARIC recognition is required.

[5] Recruited candidates shall be required to demonstrate before their first promotion the ability to work in a third EU language.

2.3. Professional experience[6]

By the deadline for applications, and in addition to the qualifications required above, candidates must have at least **five years** of relevant professional experience gained after obtaining the diploma required under 2.1.

SELECTION CRITERIA

Applications that fulfil the above Eligibility Criteria will be assessed against the following requirements:

Essential

1. At least five (5) years of proven professional experience in incident management;
2. Proven comprehensive experience in at least one of the other areas of cybersecurity such as threat intelligence, digital forensic, offensive and/or defensive cybersecurity expertise;
3. Demonstrated knowledge of SIEM tooling, including experience in writing and developing advanced threat hunting queries;
4. Thorough knowledge of information technology and practical knowledge of key components of IT infrastructure and cloud environments (AWS, Azure) and its security controls, gained through professional experience and/or training;
5. Excellent oral and written communication skills in English (CEFR level: C1 or above), including proven ability to present information in a clear and concise manner.

Advantageous

1. University degree in computing, computing science, cybersecurity, mathematics, or physics;
2. Professional certification in cybersecurity (e.g. CISM, CISSP);
3. Proven knowledge of NIST Cybersecurity framework 2.0, gained through professional experience and/or training;
4. Demonstrated expertise in ISO 27001 compliance and implementation, gained through professional experience.

Candidates invited to the test and interview phase may also be assessed against the competencies listed under the "Your key competencies" section on page 3.

[6] Professional experience will be counted from the date on which the applicant acquired the minimum qualification for access to this post. Only duly documented professional activity (i.e. remunerated employment or self-employment) is taken into account. Part-time work will be taken into account in proportion to the percentage of full-time hours worked. Periods of education or training and unremunerated traineeships are not taken into account. Completed PhDs can be counted as professional experience up to a maximum of 3 years. Any given time period can be counted only once.