European Union Agency for Cybersecurity
Agamemnonos 14
Chalandri | 15231 | Attiki Greece
Tel:+302814409711
email: info@enisa.europa.eu
www.enisa.europa.eu

CALL FOR EXPRESSION OF INTEREST FOR TRAINEESHIPS

REF. ENISA-TRA-2025-09

Type of contract	**Traineeship**
Duration of traineeship	**6 months**[1]
Area	**All of ENISA's organisational entities**
Place of Employment	**Athens, Greece or Brussels, Belgium**
Deadline for applications	**08/01/2026 at 23:59:59 hrs EET (CET**[2] **+1)**
Monthly grant	**1500**[3]

1. THE AGENCY

ENISA's mission is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, European Union institutions, industry, academia and EU citizens[4].

ENISA contributes to policy development and implementation, supports capacity building and preparedness, facilitates operational cooperation at Union level, enhances the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enables knowledge sharing, research, innovation and awareness raising, whilst developing cross-border communities and synergies.

ENISA is located in Athens, Greece (the Agency's official seat) with a branch office in Heraklion, Greece and a Local Office in Brussels, Belgium.

Further information about ENISA is available on the ENISA website: https://www.enisa.europa.eu/.

2. THE TRAINEESHIP PROGRAMME

The Traineeship Programme creates an opportunity to provide recent university graduates, including persons in the course of lifelong learning, with a unique and first-hand experience of the workings of ENISA, while the Agency benefits from the input of recent graduates, who may offer a fresh point of view and their up-to-date academic knowledge, which

[1] With the option reserved to the Agency to extend the traineeship for another period **up to 6 months,** upon justification by the Head of Unit and budget availability of the Agency.
[2] Central European Time Zone.
[3] The amount of the grant may be reviewed during the traineeship
[4] Regulation (EU) 2019/881 - Cybersecurity Act: http://data.europa.eu/eli/reg/2019/881/oj

in turn enhances the everyday work of ENISA. ENISA is an inclusive workplace and equal opportunities employer that welcomes applications from all candidates, including those with disabilities or special needs. Traineeships will be offered to candidates with the ability to participate and contribute to the extent necessary and who can benefit from the experience.

During the traineeship, Trainees may rotate within the Agency or may be involved in cross-Agency projects or be even re-allocated to another position, depending on the needs of the service and their profile and experience.

This call for traineeship positions concerns all of the Agency's organisational entities. Below, there is an overview of the core tasks the trainee is expected to perform, depending on the organisational entity they choose to apply for.

Organisational Entity	University degree required	Core tasks of the Unit
Corporate Support Services Unit (CSS)	Psychology, Human Resources, Social Sciences OR Public/Business Administration OR Law or Political Science or similar OR Facility / Sustainable management / Building Infrastructure / Security management OR Information Technology, computer science, computer engineering (electronic, telecommunications, informatics) OR Finance / Economics / Audit / or similar OR Procurement and Supply management or similar OR Statistics / (Applied) Mathematics/ Data science / Data analysis or similar	The Corporate Support Services Unit ensure seamless functioning of ENISA administrative services and support the Executive Director and all units in core activities such as but not limited to: 1. Human Resources (Talent Acquisition & Talent Management & Talent Development) 2. Budget Planning and Reporting (EU budget planning, coordination, monitoring and reporting) 3. Finance and Procurement (Contract management, financial initiation and verification, supplier management) 4. Legal Analysis & Policy Development (Staff Regulations & CEOS, Data Protection, Financial Regulations, Procurement vademecum, legal drafting and complaint handling) 5. Information Technology (Network and software, cloud, program management, digital transformation etc) 6. Security services (physical security, health and safety etc) 7. Facility & Event Management (building maintenance, sustainability, event coordination) 8. Relations with EU Institutions and EUIBAS 9. Data Analytics and Foresight on HR, Finance, IT, and overall ENISA resource planning
Executive Director's Office (EDO)	Public / Business Administration OR Law / Auditing / Political Science OR	The Executive Director's Office focuses on: 1.Policy prioritisation, Single Programming Document, Resource Planning;

Organisational Entity	University degree required	Core tasks of the Unit
	Finance / Economics / Statistics or similar OR Communications / Media / Journalism or similar OR Information Technology (with emphasis on Cybersecurity) / Computer Science OR Engineering (electronic, telecommunications, informatics) OR Library Studies OR Data Science	1. Produce reports, statistics, data analysis in terms of performance management in finance, accounting, human resources, IT, policy etc.; 2. Relations with EU Institutions, Member States and stakeholders at large; 3. Statutory Bodies of the Agency's 4. ENISA's own cybersecurity posture, performance, policy, audits and compliance including interactions with IT Systems administrators; 5. Internal Controls and Audits; 6. Document management, data management including on the intranet; 7. Website management; 8. Communications, events, relations with Press 9. Legal Clerking.
Policy Monitoring & Analyses Unit (PMA)	Public / Business Administration OR Law / Auditing OR Finance / Economics / Procurement / Statistics or similar OR Computer sciences, Informatics, Applied mathematics or similar	The Policy and Monitoring Unit focuses on: 1. Collection and analysis of knowledge on EU cybersecurity policy and national implementations; 2. Assistance to Member States in revising and implementing national cybersecurity strategies; 3. Technical advice to support cybersecurity policy development and implementation.
Resilience of Critical Sectors Unit (RoCS)	Information Technology (with emphasis on Cybersecurity) OR Computer Science (with some relevance to Cybersecurity) OR Engineering (electronic, telecommunications, informatics, space) OR Data analysis OR Political Science	The Resilience of Critical Sectors (RCS) unit focuses on: 1. Horizontal NIS2 implementation: Develop EU frameworks for NIS2 security measures, NIS2 incident reporting, NIS2 supervision and supporting the NIS Cooperation group. 2. Union risk evaluations and toolboxes: Support the 5G toolbox process, the ICT supply chain security toolbox, supporting Union stress tests. 3. Sectorial NIS2 implementation: Support a number of specific NIS2 sectors, supporting the implementation of sectorial rules, lex specialist and sectorial action plans, such as the Network code cross-border electricity flows, DORA, the Health Action plan, the Nevers recommendations. Sectors of focus: Digital infrastructures (telecom, core internet, cloud, trust), energy (electricity, gas), finance, health, transport (rail, aviation, maritime), space, public administrations. 4. Implementation check: Annual cross-sector and cross-EU cybersecurity maturity assessments, across the entire scope of the NIS2 sectors, particularly the NIS investments and the NIS360, which rely on direct information from companies in the sectors.

Organisational Entity	University degree required	Core tasks of the Unit
Capacity Building Unit (CBU)	Social sciences OR Information Technology OR Public policy/education, Pubic administration or similar	The Capacity Building Unit focuses on: 1. Empowering communities to execute their own capacity building programs using ENISA's relevant tools and methodologies (e. g. AR in a Box, Exercise Methodology) 2. Organizing specific and limited number of capacity enhancing activities (e. g. related to BLUEPRINT) to critical operational communities (e.g. Cyber Europe) 3. Helping users of ENISA tools/standards/methodologies to ensure impact, track progress and monitor results 4. Promote adoption of ECSF, maintain and regularly review ECSF, pilot an attestation mechanism for specific profile(s) of ECSF
Operational Cooperation Unit (OCU)	Information Technology (with emphasis on Cybersecurity)	The Operational Cooperation Unit (OCU) serves as an enabler and empowers the cooperation of CSIRTs Network, CyCLONe and all actors involved in the EU to collaborate and respond to large scale incidents and crises by providing the best tools and support in order to: 1. Enhance and improve incident response capabilities and readiness across the Union through CSIRTs Network 2. Enable effective European cybersecurity crisis management via CyCLONe 3. Ensure coordination in cybersecurity crisis management among relevant EU institutions, bodies and agencies (e.g. CERT-EU, EEAS, EUROPOL) 4. Improve maturity and capabilities of operational communities (CSIRTs Network, CyCLONe and EUIBAs) including cooperation with Law enforcement 5. Contribute to preparedness, shared situational awareness, coordinated response and recovery to large scale cyber incidents and crises across different communities 6. Support the evolution of EU joint response by enabling the deployment of EU level proposals. Provide tools and infrastructures to the CSIRTs Network, CyCLONe and all actors involved in the EU cybersecurity
Operational & Situational Awareness Unit (OSA)	Information Technology (with emphasis on Cybersecurity) / Computer Science OR Engineering (electronic, telecommunications, informatics) OR Data analysis OR Geopolitics / Russian Studies / Chinese Studies	The Operational & Situational Awareness Unit comprises of two sectors a) Threat Analysis Service (TAS) and b) Incidents and Vulnerabilities Service (IVS) and focuses on: 1. contributing to cooperative preparedness and response at Union and Member States level, through data driven threat and risk analysis, 2. operational and strategic recommendation based on collection of incidents, vulnerability and threat information to contribute to the Union common situational awareness.

Organisational Entity	University degree required	Core tasks of the Unit
Operational Support Unit (OSU)	Information Technology (with emphasis on Cybersecurity)	The Operational Support Unit focuses on: 1. implementing the EU Cybersecurity Reserve under the Cyber Solidarity Act (CSoA) offering support to EU Member States and EU Institutions Bodies and Agencies in order to respond to effectively to large scale cybersecurity incidents and crises. 2. Support preparedness activities for the improvement of the cybersecurity posture of beneficiaries in order to face effectively future cybersecurity incidents.
Cybersecurity Certification Unit (CCU)	Computer Science / Computer Engineering / Information Technology / Information Science OR Electronic / Electrical Engineering OR Telecommunications (with focus on cybersecurity)	The Cybersecurity Certification Unit focuses on: 1. establish and support the EU cybersecurity certification framework in accordance with Article 49 of the CSA; 2. Assist ENISA with EU certification schemes, technical documents, and managing Working Groups; 3. Provide assurance on digital solutions for trusted supply chains. 4. Develop cryptography guidelines within the ECCG subgroup. 5. Help MSs in building national certification strategies and capacities. 6. Analyse aspects of relevant legislative instruments related to certification
Market, Technology and Product Security Unit (MTPS)	Computer Science / Computer Engineering/ Information Technology / Information Science OR Electronic / Electrical Engineering OR Telecommunications (with focus on cybersecurity)	The Market, Technology and Product Security Unit focuses on: 1. Enhance ENISA's role in the CRA through market analysis, market sweeps, and identification of emerging cybersecurity risks; 2. Collaborate with market authorities to align relevant requirements defined by the CRA; 3. Provide analyses and guidelines on cybersecurity and data protection, supporting compliance with standards like eIDAS2. 4. Promote and implement 'security by design' and 'security by default' measures in ICT products and services, encouraging standardization and codes of conduct; 5. Promote understanding of cybersecurity trends in strategic EU sectors through foresight activities. 6. Support cybersecurity certification and conformity assessment in alignment with European standards 7. Perform market trend analysis, monitoring vulnerabilities in ICT products and processes.

3. QUALIFICATIONS AND EXPERIENCE REQUIRED[5]

3.1 ELIGIBILITY CRITERIA

The selection procedure is open to candidates, who satisfy the following eligibility criteria on the closing date and time for applications:

1. Nationality

Trainees have to be nationals of the Member States of the European Union or the European Free Trade Association (EFTA), unless an exception is authorized by the appointing authority, and enjoy their full rights as citizens.

2. Qualifications

(a) University Diploma

Candidates must have completed a university-level education of at least 3 years[6] and obtained a full bachelor degree or its equivalent by the closing date for applications. For an indicative list of minimum national qualifications required by the legislation in the country where the diploma was obtained, see the website of EPSO at the following link (point 3.1 in the list applicable to the relevant Member State): https://epso.europa.eu/documents/2392.

(b) Languages

In order for the Trainee to fully profit from the traineeship and to be able to follow meetings and perform adequately, they must have very good knowledge of at least two EU languages, of which one should be the main working language of ENISA (English).

3.2 SELECTION CRITERIA

Only eligible candidates, who fulfil the above eligibility criteria, will be further assessed against the selection criteria, solely based on the information provided by the candidates in their application form and the talent screening questions. Candidates must provide concrete examples of how they fulfil the below criteria in their application form.

Candidates must demonstrate and will be assessed on the following criteria:

- Completed University Degree[6] in one of the areas mentioned next to the corresponding Organisational entity/entities the applicant is applying for (see table Section 2);
- Ability to take initiative, take responsibility for specific tasks and follow through, with the ability to work effectively both independently and as part of a team;
- Aptitude for working with Microsoft Office applications and/or Information Systems;
- Good communication and interpersonal skills, with a strong sense of commitment;
- Motivation to work in a multidisciplinary, multicultural and fast-paced environment.

In addition, successful candidates should act and abide by ENISA's core values. An outline of the ENISA's core values as well as a full description of the **ENISA's competencies** is available here.

NB: Candidates are advised to demonstrate with concrete examples in their application how they fulfill the above criteria.

[5] Candidates must satisfy ALL the eligibility criteria on the closing date of the application. In the event that you do not fulfil all the eligibility criteria, your application will not be further assessed. Candidates should assess and check before submitting their application whether they fulfil all the requirements as specified in the vacancy notice. Please include in the application form only professional experience and academic qualifications for which you hold supporting documents. Candidates must be able to provide supporting documents clearly showing duration and nature of experience upon request.

[6] Only diplomas issued by EU Member State authorities and diplomas recognised 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 recognised 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. For diplomas awarded in the UK diplomas awarded until 31/12/2020 are accepted without further recognition. For diplomas awarded after this date (from 01/01/2021), a NARIC recognition is required: https://www.enic-naric.net/. Candidates must meet this requirement on the closing date of application.

4. SUBMISSION OF APPLICATIONS

To apply for this vacancy, please use ENISA's e-recruitment system, complete all required sections of the application and submit it. ENISA does not accept applications submitted by e-mail, mail or any other means. The application must be submitted in the English language, which is the working language of ENISA.

Candidates must send their application within the set deadline. In order to be considered, applications must be received by **23:59:59 EET[7] (Greek time (CET[8]+1))** on the closing date. Once you have submitted your application, you will receive an automatic e-mail message confirming receipt of your application. Please ensure that the email address you provide for your applicant account is correct and that you check your email and spam/junk folders regularly.

Applicants are strongly advised to submit their applications well in advance of the deadline, since heavy internet traffic or fault with the internet connection could lead to difficulties in last minute submission. ENISA cannot be held responsible for any delay related to internet connection issues etc.

At this stage of the selection procedure candidates are not required to send any additional supporting documents with the application (i.e.: copies of ID-card, educational certificates, evidence of previous professional experience etc.).

5. SELECTION PROCEDURE

The organizational entities will assess applications solely based on the information provided by candidates in their application form.

Applicants are selected on the basis of a review of their application and a phone or video interview, which shall take into account the suitability of the person for the position and their qualifications. The Agency strives to maintain a balanced geographical origin of staff, interims and Trainees and will take this aspect into account as well.

Successful candidates are selected on the basis of their educational background, qualifications, competences, and motivation and/or experience. The selection procedure aims to establish a diverse pool of shortlisted candidates to the best possible degree.

Selected Trainees are obliged to provide documentary proof of their eligibility, qualifications and any supporting documents and certificates required by Human Resources, within the indicated deadline. They are responsible for making sure that they obtain all the documentation required by the national authorities, if necessary.

All trainees must possess valid health insurance for Greece or Belgium throughout the entire period of their traineeship. No later that one week before the start date of the traineeship, the trainee should present the proof of this insurance to the HR Unit. The costs related to this compulsory health insurance are not covered by ENISA. Trainees are also advised to establish a civil liability insurance.

More details about the traineeship programme in ENISA can be found here.
For any questions on the recruitment process or other technical issues, feel free to reach out via email to recruitment@enisa.europa.eu.

[7] Eastern European Time
[8] Central European Time

6. EQUAL OPPORTUNITY

As a European Union Agency, ENISA is committed to providing equal opportunities to all its employees and applicants for employment. As an employer, ENISA is committed to ensuring gender equality and to preventing discrimination on any grounds. It actively welcomes applications from all qualified candidates from diverse backgrounds, across all abilities, without any distinction on any ground such as sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age, marital status or other family situation or sexual orientation, and from the broadest possible geographical basis amongst the EU Member States. In particular, ENISA encourages the applications of women for the positions where they are currently under-represented.

If you have a disability or medical condition that may hinder ability to sit the interview or written test, please indicate this in your application and let us know the type of special arrangements you need. If the disability or medical condition is developed after the deadline for the applications, you must notify us via email recruitment@enisa.europa.eu. Overall, ENISA strives to select, recruit, develop and retain, diverse talent workforce.

7. DATA PROTECTION

All personal data shall be processed in accordance with Regulation (EU) No 2018/1725 of the European Parliament and of the Council (OJ L 295, 21.11.2018, p. 39–98) 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 data. ENISA is supervised by EDPS, http://www.edps.europa.eu . For any further enquiries you may contact the Data Protection Officer at: dataprotection@enisa.europa.eu.

Candidates are invited to consult the privacy statement which explains how ENISA processes personal data in relation to recruitment selections.