European Union Agency for Cybersecurity
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711 | e-mail: info@enisa.europa.eu
www.enisa.europa.eu

CALL FOR APPLICATIONS: ENISA'S AWARENESS RAISING AND CYBER-HYGIENE AD-HOC WORKING GROUP

1. INTRODUCTION

The **Awareness Raising and Cyber-Hygiene Ad-Hoc Working Group (AHWG)** will aim at supporting the European Union Agency for Cybersecurity (ENISA) to foster a culture of cybersecurity awareness and promote strong cyber hygiene practices across Europe. As stated in the findings of the '2024 Report on the state of cybersecurity the Union'[1], people's confidence in their ability to protect themselves from cybercrime decreased, while their awareness about cybercrime and relevant reporting mechanisms among EU population, is low.

The policy recommendation of the afore-mentioned report is, thus, to promote a unified approach by building on existing policy initiatives and by harmonising national efforts to achieve a common high-level of cybersecurity awareness and cyber hygiene among professionals and citizens, irrespective of demographic characteristics. In an increasingly interconnected world, where cyber threats continue to evolve and grow in sophistication, raising awareness and equipping individuals, organizations, and institutions with the knowledge and tools to protect themselves is more critical than ever.

The NIS2 Directive mentions that awareness raising and basic cyber hygiene practices and cybersecurity training' are part of the minimum measures that Member States shall ensure both for citizens and for essential and important entities to prevent or minimize the impact of incidents on recipients of their services and on other services. Moreover, the Member States shall also aim at strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of the Directive, by providing easily accessible guidance and assistance for their specific needs'.[2]

[1] 2024 Report on the State of the Cybersecurity in the Union, available online at:https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf.
[2] Art 7 (2-i); Art 21(2-g) - Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available online at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj[3] Commission unveils action plan to protect the health sector from cyberattacks available at: https://digital-strategy.ec.europa.eu/en/news/commission-unveils-action-plan-protect-health-sector-cyberattacks

In addition, on 15 January 2024, the Commission launched a European action plan to strengthen the cybersecurity of hospitals and healthcare providers a sector currently receiving political attention due to recent attacks but also due to the criticality it entails. Part of the Political Guidelines of the 2024-2029 Commission mandate, the action plan focuses on improving threat detection, preparedness, and crisis response in the healthcare sector. It aims to provide tailored guidance, tools, services, and training to hospitals and healthcare providers. The action plan proposes, among others, for ENISA, the EU agency for cybersecurity, to establish a pan-European Cybersecurity Support Centre for hospitals and healthcare providers, providing them with tailored guidance, tools, services, and training[3].

Along these lines, ENISA seeks to interact with a broad range of stakeholders for the purpose of supporting the efforts on elevating the base-level of cybersecurity awareness and hygiene across the EU. The membership to the AHWG is foreseen to pursue broad, interdisciplinary representation across stakeholders' communities.

The group, supported by ENISA, will bring together professionals from diverse sectors, including public and private organizations, academia, civil society, and cybersecurity experts. It will serve as a platform for collaboration, knowledge-sharing, and the co-creation of impactful initiatives that address the unique challenges of cybersecurity awareness across Europe's diverse cultural, linguistic, and technological landscape.

2. BACKGROUND OF THE ADHOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881, Art. 20[4], the Executive Director of the EU Agency for Cybersecurity may set up ad hoc-working groups (AHWGs) composed of experts where necessary and within ENISA's objectives and tasks. Adhoc working groups provide ENISA with specific advice and expertise. Prior to setting up an ad-hoc working group, the Executive Director of ENISA shall inform the agency's Management Board.

The members of the ad-hoc working groups are selected according to the highest standards of expertise, aiming to ensure appropriate balance according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector, including industry, users, and academic experts in network and information security[5].

Regulation (EU) 2019/8814 (Art. 10)[6], stipulates ENISA's activities with regards to awareness raising and cyber-hygiene education. Moreover, ENISA's Single Programming Document 2025-2027[7] (Activity 3) highlights the need for dedicated capacity building activities towards awareness raising and cyber-hygiene and their promotion. Under this activity ENISA plans to improve the capabilities of Member States, EU entities, as well as public and private stakeholders from NIS2 Sectors. It focuses on improving stakeholders' resilience and response capabilities, enhancing their skills and attitude with regards to cyber hygiene, and increasing their preparedness.

Under this activity ENISA plans to facilitate and empower targeted communities of stakeholders to leverage the tools, platforms and frameworks developed by ENISA. The group will support the development, deployment and promoton of awareness raising tools, frameworks and content that enable stakeholders, in particular NIS2 sectors, to independently execute their own cyber-hygiene training or awareness raising programmes. In this effort, ENISA will

[3] Commission unveils action plan to protect the health sector from cyberattacks: https://digital-strategy.ec.europa.eu/en/news/commission-unveils-action-plan-protect-health-sector-cyberattacks.
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881
[5] Idem.
[6] Idem.
[7] ENISA's Single Programming Document 2025-2027, available at: https://www.enisa.europa.eu/publications/enisa-single-programming-document-2025-2027

take stock of existing programmes and initiatives that are ongoing and establish synergies, for example with other European Institutions and recognized bodies, avoiding duplication of activities.

3. SCOPE OF THE ADHOC WORKING GROUP

The scope of this Awareness Raising and Cyber-Hygiene ad-hoc working group (ARCH - AHWG) is to advise and support ENISA in cybersecurity awareness raising and cyber-hygiene activities to ensure cybersecurity best practices adoption.

The group will engage in a wide range of activities to achieve its mission of raising cybersecurity awareness and promoting strong cyber hygiene practices across Europe, while also facilitating and empowering targeted communities of stakeholders to upskill and reskill cybersecurity professionals in line with the ENISA Strategy[8] and international context[9].

In particular, ENISA **would like to focus but not limit** the activities around its frameworks and services, such as the AR-in-a-BOX[10]. These activities are designed to develop and support communities that will facilitate and multiply the sharing of frameworks, good practices and lessons learnt.

3.1 KEY TASKS OF THIS AD-HOC WORKING GROUP

Key tasks of the ad-hoc working group include, and are not limited to, the following:

- Advise ENISA through expert counsel in carrying out its tasks concerning cybersecurity awareness raising and community empowerment;
- Review of deliverables/documentation deriving from the ENISA projects;
- Support ENISA in specific activities for designing, developing, providing, promoting and evaluating cybersecurity awareness raising campaigns and cyber-hygiene best practices, along with high impact events.

ENISA may engage with the whole group for these tasks and/or with specific experts from within the group (or the reserve list of the group) depending on the specific requirements and needs of the Agency.

Example of activities that the members of this group might undertake:

AWARENESS PROGRAMS

Objective: Undertake a multiplier's role to amplify the usage of ENISA's tools, frameworks and methodologies, such as promoting the AR-in-a Box related services to their constituency.

WORKSHOPS

Objective: Provide hands-on learning opportunities to improve cybersecurity skills among individuals and organizations, focusing primarily on ENISA's tools and methodologies and in specific the methodology of AR-in-a Box. In the future contributors from this group could prepare content to be distributed.

[8] 'A trusted and cybersecure Europe - ENISA strategy', available at: https://www.enisa.europa.eu/sites/default/files/2025-02/A%20Trusted%20and%20Cyber%20Secure%20Europe%20-%20ENISA%20Strategy.pdf
[9] 'International strategy of the EU Agency for cybersecurity', available at: https://www.enisa.europa.eu/sites/default/files/all_files/2022-02-16%20ENISA%20International%20Strategy.pdf
[10] 'Cybersecurity Awareness Raising: The ENISA-Do-It-Yourself Toolbox', available at: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box

TRAINING SESSIONS

Objective: Build capacity in their community; act as ambassadors, trainers or multipliers in their own networks.

RESOURCE DEVELOPMENT

Objective: Create high-quality cyber awareness and hygiene materials to support efforts across Europe.

COLLABORATIVE PROJECTS

Objective: Foster innovation and cooperation among community members to address shared challenges in cybersecurity awareness.

PUBLIC ENGAGEMENT EVENTS

Objective: Strengthen connections between their community and the general public while promoting cybersecurity hygiene awareness.

3.2 MONITORING AND FEEDBACK MECHANISMS

Monitoring and feedback mechanisms are necessary in order to achieve continuous improvement of activities based on measurable outcomes and participant feedback.These mechanisms will be discussed and decided at the kick-off meeting of the group based upon a proposal of ENISA.

4. SELECTION AND APPOINTMENT OF MEMBERS AND OBSERVERS

The ARCH-AHWG will be composed of up to 25 selected members-leading experts, based on the requirements of this open call. The preliminary estimate of the duration of the ad-hoc working group is for up to two (2) calendar years from the issue of the respective Agency Decision that signals the kick-off date of this working group's operation; extension of the mandate of this working group is possible should the scope of the work is not completed in two years.

Annually, a total workload of up to 15 working days is foreseen according to the role each member will undertake. The frequency of interaction will be decided between ENISA and the members of the group.

The Members, including those in the reserve list, may be requested by the Agency for further or specific engagement upon remuneration (see Article 8 of this Call).

For a balanced composition of the AHWG, ENISA will take into account factors such as: relevance and public visibility of profile to carry-out the afore-mentioned activities, sector, geographical and gender balance among selected members to cover various stakeholder groups both from the cybersecurity and communications field in the private, academia, and civil society organisations. Priority will be given to profiles that are actively engaged in the NIS2 sectors.

The members of this ad-hoc working group may be reimbursed for their expenses to participate in the meetings according to the ENISA internal rules for reimbursement. Members may be also subject to remuneration in case they undertake specific tasks, in line with ENISA's policy on remunerated external experts.

Besides members of the ad-hoc working group, ENISA is likely to appoint a reserve list, in accordance with the same conditions that apply to members, who shall be called to replace any members who are absent or otherwise indisposed. In case of a member's unavailability, disqualification or resignation, the chair of the ad hoc working group can appoint a member (or members) from the reserve list, to replace any members who are indisposed. The new member(s) will be appointed for the remaining of the term of the ad hoc working group.

Members who are no longer capable to contribute effectively to the group's deliberations, who in the opinion of ENISA do not comply with the conditions set out in Article 339[11] of the Treaty on the functioning of the European Union or who resign, shall no longer be invited to participate in any meetings of the Group and may be replaced for the remaining duration of the ad-hoc working group.

ENISA will propose to the ad hoc working group a set of draft rules of procedure to be adopted as appropriate.

The AHWG established through this call shall, as appropriate, include experts - apart from the private sector, academia and civil society sectors mentioned above- also from the public administrations of the Member States and EEA/EFTA States, as well as from the European Union institutions, bodies, offices and agencies (EUIBAs).. Representatives of the various organisations and bodies, mentioned above can join meetings as observers.

In addition, representatives of international organisations and consumer associations may be invited by the Chairperson to participate in meetings of the AHWG. Such participants are not considered as appointed members of the AHWG and will bear their own expenses.

5. ORGANISATION OF THE AD HOC WORKING GROUP

A member of the ENISA staff will be designated by the ENISA Executive Director as Chairperson of the AHWG. If necessary, a Vice-Chairperson(s) from ENISA staff might also be designated. The Secretariat of the AHWG will be provided by ENISA to the AHWG. The governance of the group and roles will be decided in collaboration with the selected members.

The Chairperson convenes the meetings of the working group, administers the agenda of the meeting, ensures a timely distribution of information and documents to all working group members and addresses all organisational aspects to facilitate the smooth functioning of the working group. The agenda of the meeting will be provided ultimately 4 working days before the start of the meeting.

The AHWG may be divided into Thematic Groups based upon the different areas of work that will be developed along the project phases. If during the development of the work of the AHWG Thematic Groups are deemed necessary, AHWG members will be invited to participate in the Thematic Group on the basis of their interest and expertise.

In principle, the AHWG shall convene online, in ENISA premises or as otherwise decided on a proposal of the Chairperson. The bulk of the work would be carried out remotely; conference calls or video conferencing are permitted and encouraged for exchanges between members.

Support and planning as well as secretariat service will be provided by ENISA, as appropriate. More specifically, ENISA will be responsible for the organisation of the work and support of the working group.

ENISA shall ensure interaction and/ or consultation with the other ENISA advisory bodies, and/ or other stakeholders throughout the lifespan of the AHWG, as appropriate.

[11] Consolidated version of the Treaty on the Functioning of the European Union PART SEVEN - GENERAL AND FINAL PROVISIONS Article 339 (ex Article 287 TEC) available at: https://eur-lex.europa.eu/eli/treaty/tfeu_2016/art_339/oj/eng

ENISA will organise plenaries of the full AHWG with a minimum of four (4) meetings per calendar year. There might be more frequent meetings of the different Thematic Groups established to support dedicated work streams.

6. CONFIDENTIALITY AND DECLARATIONS OF INTEREST

The members of the AHWG, as well as invited experts and observers, are subject to the obligation of professional confidentiality according to Article 27 of Regulation (EU) 2019/881[12]. More specifically, members of the AHWG shall comply with the confidentiality requirements of Article 339 TFEU[13], even after their duties have ceased. Each member shall sign a confidentiality statement for the duration of the activity.

Documents produced under the establishment and operation of the AHWG may be subject to the conditions of Regulation (EC) No 1049/2001 on public access to documents[14].

When members of the AHWG are invited to bring forward their views on aspects or topics related to the work of the AHWG, they may need to be able to consult with their organisations or parties related to them outside their organisation to the extend necessary. They likewise need to be able to share information within their organisation or other relevant parties on a need-to-know-basis, unless the information is indicated in writing, or by announcement of the (Vice)-Chairperson as confidential. Information produced by the AHWG can only be made public upon prior approval of the Chairperson.

After ENISA has published the list of appointed AHWG members, the AHWG members may disclose their membership in this AHWG to the public and describe the general scope of the work of the AHWG.

In addition, the members of the AHWG are subject to the obligations of Article 25(2) of Regulation (EU) 2019/881[15] related to declaration of interests.

7. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[16].

For further information, please refer to the data protection notice that is available as a separate document with the call, as well as the record of data processing activities for ENISA AdHWs[17]

[12] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881
[13] Consolidated version of the Treaty on the Functioning of the European Union PART SEVEN - GENERAL AND FINAL PROVISIONS Article 339, available at:https://eur-lex.europa.eu/eli/treaty/tfeu_2012/art_339/oj/eng
[14] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Available online at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32001R1049.
[15] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881
[16] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC. Available online at: https://eur-lex.europa.eu/eli/reg/2018/1725/oj.
[17] Record-40-Ad-Hoc-Working-Groups-Call-for-Expression-of-Interest-Appointment-Operation.pdf

8. REIMBURSEMENT OF MEMBERS

8.1 REIMBURSEMENT OF THE AHWG MEMBERS FOR THEIR TRAVEL AND SUBSISTENCE EXPENSES IN CONNECTION WITH THE ACTIVITIES OF THE AHWG

The members of the AHWG may be reimbursed for their travel and subsistence expenses in connection with the activities of the working group subject to the availability of funds. If a member comes from a location different than the location required for the provision of services, or the place of the meeting, the following expenses are then eligible:

1. Travel expenses (economy class flight or 1st class train – whichever is more cost-effective) from the city in which the member is officially registered to the location required for the provision of services, or the place of the meeting.[18]
2. A "daily subsistence allowance (DSA)" applicable to the country in which the meeting will take place. This allowance is set by the European Commission[19] and it covers all daily living expenses including hotel, meals, local travel etc.
3. No other claims for living or transportation costs will be accepted.

Members may select to refrain from being reimbursed on the basis of personal or professional considerations; in this case they remain eligible to apply.

Representatives of Member States and observers are neither remunerated nor reimbursed, except in duly justified cases, to be determined by the Chairperson of the AHWG.

8.2 REIMBURSEMENT OF THE AHWG MEMBERS FOR ADDITIONAL TASKS

Members of the AHWG and of the AHWG reserve list that are citizens or permanent residents of the EU or EEA of the EU or EEA, may be engaged in additional tasks conducted within or outside the scope of AHWG activities. In such case, the members of the AHWG (and of the reserve list) shall be eligible for reimbursement under the same rules and procedures as those applicable for the ENISA CEI list of experts[20]. The remuneration shall be based on the thresholds defined under Article 242 of the Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (Financial Regulation)[21] and under the following rules:

- The remuneration of the experts engaged from the list of the AHWG members shall be based on days of engagement and with a fixed daily fee of 450 euro[22].
- The annual remuneration of a single expert shall in principle not exceed 30.000 euro.
- The maximum amount of fees that can be paid to a single expert shall be 90 000 euro during a period of four consecutive calendar years.

AHWG members engaged by ENISA as remunerated experts may also be entitled to the reimbursement of expenses incurred in the course of journeys if invited to meetings organised by ENISA. In such case, the provisions of point 8.1 shall apply.

[18] Each invitee, to be eligible for the reimbursement, needs to have their Legal entity and Financial Identification validated on the European Commission's central data base, available under following link: Forms for contracts - European Commission.
[19] The latest rates are available to download from: https://international-partnerships.ec.europa.eu/document/download/16b30948-4166-4846-98bb-aa055be5fd75_en?filename=Per%20diem%20rates%20-%2025%20July%202022.pdf.
[20] CEI List of Individual External Experts to Assist ENISA | ENISA
[21] Regulation - EU, Euratom - 2024/2509 - EN - EUR-Lex.
[22] This is the maximum amount indicated in the Commission Decision establishing horizontal rules on the creation and operation of Commission expert groups C (2016) 3301 final.

If the applicants for the AHWG wish to be considered for additional remunerated tasks, they need to submit additional documents, namely proof of EU/EEA citizenship or permanent residence and proof of having a bank account in the EU member state or EEA. They shall indicate it clearly in their application form, shall this be the case. They must also provide a declaration on their honour, in accordance with the template in Annex 1 to the present Call for expression of interest, duly signed and dated, stating that they are not in one of situations of exclusion as per criteria set out in the Article 138 of the Financial Regulation.

The validity period of the list of AHWG members (and reserve list) that may be considered for additional remunerated tasks shall follow the validity of the established AHWG.

8.3 TRANSPARENCY: EX-POST INFORMATION

If an expert has concluded a contract of more than 15.000 EUR, the name, the locality (region of origin), amount and subject of the contract shall be published on the website of the contracting authority no later than 30 June of the year following the contract award. The information shall be removed two years after the year of the contract award.

9. APPLICATION PROCEDURE

Individuals interested in becoming members of this AHWG are invited to submit their application to ENISA using the application form[23], available in the dedicated section on the ENISA website. An application will be deemed admissible only if it is submitted by the deadline.

Public entities and organisations that represent a common interest and generally serve a public goal may apply to become permanent observers in the group. They should submit their interest explaining their motivation and the public goal. They will also need to include the name of the proposed permanent representative. The application must be submitted to Executive Director and sent to Awareness@enisa.europa.eu.The Executive Director may accept the participation of the organisation and their representative as observer of the working group.

The list of appointed members and permanent representatives will be made public in the ENISA website.

9.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted **by 11 July 2025 at 12:00 EET (Athens time zone)**. The date and time of submission will be established on the ENISA website, used to collect all submitted applications,[24] upon submission of an application.

10. TERMINATION OF THE MANDATE OF THE AD-HOC WORKING GROUP AND DISSOLUTION

At the moment the tasks of the AHWG are completed, the end-of-life phase of the AHWG will follow. ENISA reserves the right to terminate the AHWG at any moment if there is not anymore a need for such AHWG.

[23] https://www.enisa.europa.eu/working-with-us/ad-hoc-working-groups-calls/enisas-awareness-raising-and-cyber-hygiene-ad-hoc-working-group/apply

11. ELIGIBILITY CRITERIA

Based on the self-declared application forms received, only candidates who meet the following minimum criteria will automatically be considered to be included in the list of external experts dependent on endorsement by an evaluation committee:

1. Have fully completed their application form;
2. Are a national of, or working for a legal entity of one of the Member States of the EU or EEA;
3. Have a bank account in an EU Member State or EEA;
4. Have proven experience in using English as a working language for a minimum of 2 years;
5. Have minimum 3 years of experience in the selected areas and fields of expertise;
6. Have minimum 12 months of experience in the selected areas and fields of expertise during the last 5 years;
7. A motivation letter (500 words maximum), which establishes your incentive to be accepted as an expert for ENISA, as well as the capability of the applicant to work with others in a multicultural environment;
8. Information on education and professional experience as well as relevant experience in the tasks involved.

The evaluation committee may exceptionally further consider candidates who are close to the minimum requirements for years of experience or who have a unique skillset, for inclusion in the List.

12. SELECTION CRITERIA

The selection of members is based on a personal capacity and a clear demonstrable skillset or research capacity in areas such as, cyber-hygiene and awareness programs in critical infrastructure protection, cyber-hygiene and awareness programs and trainings for the private and public sector, community development skills and experience, experience in developing and maintaining a stakeholders strategy, stakeholders management, promotional material development, communication strategy implementation and development, media and social media marketing skills, cyber hygiene educational material design and development skills.

In the assessment of the applications, ENISA will take into consideration the following essential criteria:

1. Relevant competence (e.g. technical, operational, legal, research, organisational or a combination thereof) and experience in the area of cybersecurity training and awareness raising and/or in other areas of relevance for the purpose of acting as multipliers and providing support and advice on the activities mentioned in the scope of the AHWG (section 3 of this Call);
2. Knowledge of methodologies and ability to deliver advise related to community building, communication, transnational campaigning, stakeholders' engagement in the cyber-security domain and in general Experience based on geographical coverage (assessed on the expertise at national, EU and/or international levels);
3. Ability to deliver technical advice on issues relevant to cybersecurity best practices in cyber-hygiene and Awareness Raising campaigns and educational programs in critical sectors (NIS2);
4. Ability to deliver advise on social media marketing and audience growth;Ability to adjust messages for different target audiences and specific communication tools;
5. Expertise with corporate branding (i.e. campaigns for public and private organisations);

Advantageous :

6. Having a wide range of contacts in their organisation, sector and beyond. Acting as a point of contact for a large community is highly appreciated.
7. Being awareness raising and cyber-hygiene trainers in their respective organisations.

8. Having completed the AR-in-a-Box training (EU ACADEMY LINK).
9. Expertise in preparing briefing notes for internal and external purposes

Applicants shall have experience in at least one of the above-mentioned essential criteria (1 to 5).

13. SELECTION PROCEDURE

The selection procedure shall consist of an assessment of the applications performed by ENISA as appropriate against the selection criteria mentioned above under point 12 of the Call (1 to 5), followed by the establishment of a list of the most suitable experts and concluded by the appointment of the members of the AHWG by the Executive Director of ENISA.

ANNEX 1

DECLARATION OF HONOUR ON EXCLUSION CRITERIA (FOR THE CANDIDATES WISHING TO BE CONSIDERED FOR ADDITIONAL TASKS AS REMUNERATED EXPERTS)

Name:

"I hereby solemnly declare that I am not in one of the following situations:

I – SITUATION OF EXCLUSION CONCERNING THE PERSON

(1) **declares that** the above-mentioned person is in one of the following situations:	YES	NO
(a) it is bankrupt, subject to insolvency or winding-up procedures, its assets are being administered by a liquidator or by a court, it is in an arrangement with creditors, its business activities are suspended or it is in any analogous situation arising from a similar procedure provided for under EU or national laws or regulations;	☐	☐
(b) it has been established by a final judgement or a final administrative decision that the person is in breach of its obligations relating to the payment of taxes or social security contributions in accordance with the applicable law;	☐	☐
(c) it has been established by a final judgement or a final administrative decision that the person is guilty of grave professional misconduct by having violated applicable laws or regulations or ethical standards of the profession to which the person belongs, or by having engaged in any wrongful conduct which has an impact on its professional credibity where such conduct denotes wrongful intent or gross negligence, including, in particular, any of the following:		
(i) fraudulently or negligently misrepresenting information required for the verification of the absence of grounds for exclusion or the fulfilment of selection criteria or in the performance of a contract or an agreement;	☐	☐
(ii) entering into agreement with other persons with the aim of distorting competition;	☐	☐
(iii) violating intellectual property rights;	☐	☐

(iv) unduly influencing or attempting to unduly influence the decision-making process to obtain Union funds by taking advantage, through misrepresentation, of a conflict of interests involving any financial actors or other persons referred to in Article 61(1) FR;	☐	☐
(v) attempting to obtain confidential information that may confer upon it undue advantages in the award procedure*;*	☐	☐
(vi) incitement to discrimination, hatred or violence against a group of persons or a member of a group or similar activities that are contrary to the values on which the Union is founded enshrined in Article 2 TEU, where such misconduct has an impact on the person's integrity which negatively affects or concretely risks affecting the performance of a contract or an agreement;	☐	☐
(d) it has been established by a final judgement that the person is guilty of the following:		
(i) fraud, within the meaning of Article 3 of Directive (EU) 2017/1371 and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995;	☐	☐
(ii) corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 and Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, drawn up by the Council Act of 26 May 1997, and conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA, as well as corruption as defined in the applicable law;	☐	☐
(iii) conduct related to a criminal organisation, as referred to in Article 2 of Council Framework Decision 2008/841/JHA;	☐	☐
(iv) money laundering or terrorist financing, within the meaning of Article 1(3), (4) and (5) of Directive (EU) 2015/849 of the European Parliament and of the Council;	☐	☐

(v) terrorist-related offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA, respectively, or inciting, aiding, abetting or attempting to commit such offences, as referred to in Article 4 of that Decision;	☐	☐
(vi) child labour or other offences concerning trafficking in human beings as referred to in Article 2 of Directive 2011/36/EU of the European Parliament and of the Council;	☐	☐
(e) it has shown significant deficiencies in complying with the main obligations in the performance of a contract or an agreement financed by the Union's budget, which has led to its early termination or to the application of liquidated damages or other contractual penalties, or which has been discovered following checks, audits or investigations by a contracting authority, the European Anti-Fraud Office (OLAF), the Court of Auditors or the European Public Prosecutor's Office (EPPO);	☐	☐
(f) it has been established by a final judgment or final administrative decision that the person has committed an irregularity within the meaning of Article 1(2) of Council Regulation (EC, Euratom) No 2988/95;	☐	☐
(g) it has been established by a final judgment or final administrative decision that the person has created an entity under a different jurisdiction with the intent to circumvent fiscal, social or any other legal obligations in the jurisdiction of its registered office, central administration or principal place of business.	☐	☐
(h) (*only for legal persons*) it has been established by a final judgment or final administrative decision that the person has been created with the intent provided for in point (g).	☐	☐
(i) for the situations referred to in points (c) to (h) above the person is subject to: i. facts established in the context of audits or investigations carried out by the European Public Prosecutor's Office after its establishment, the Court of Auditors, the European Anti-Fraud Office (OLAF) or the internal auditor, or any other check, audit or control performed under the responsibility of an authorising officer of an EU institution, of a European office or of an EU agency or body; ii. non-final administrative decisions which may include disciplinary measures taken by the competent supervisory	☐	☐

	body responsible for the verification of the application of standards of professional ethics;		
iii.	facts referred to in decisions of entities or persons being entrusted with EU budget implementation tasks;		
iv.	information transmitted by Member States implementing Union funds;		
v.	decisions of the Commission relating to the infringement of Union competition law or of a national competent authority relating to the infringement of Union or national competition law; or		
vi.	informed, by any means, that it is subject to an investigation by the European Anti-Fraud office (OLAF): either because it has been given the opportunity to comment on facts concerning it by OLAF, or it has been subject to on-the-spot checks by OLAF in the course of an investigation, or it has been notified of the opening, the closure or of any circumstance related to an investigation of the OLAF concerning it.		

Name and Surname:

Date: **Signature:**