

Memorandum of understanding

between:

The CyberHubs – European Network of Cybersecurity Skills Hubs project
(hereinafter referred to as the “CyberHubs project”),

and

[Name of CyberHubs Associated Partner]
(hereinafter referred to as the “CyberHubs Associated Partner”),

(hereinafter referred to individually as a “Party” and collectively as the “Parties”)

PREAMBLE

This Memorandum of Understanding (MoU) is set up between the CyberHubs project and the CyberHubs Associated Partner, whereas:

A. The CyberHubs project is an EU-funded project coordinated by DIGITALEUROPE under the grant agreement n 101140030 – CyberHubs - ERASMUS-EDU-2023-PI-ALL-INNO, aiming to strengthen the European cybersecurity skills ecosystem through the establishment of a sustainable network of national Cybersecurity Skills Hubs, addressing skills shortages, gaps, and mismatches.

B. The CyberHubs Associated Partner is an organisation active in the field of cybersecurity skills development, education and training, workforce development, digital skills, or closely related domains.

C. The Parties share a common interest in enhancing cooperation on cybersecurity skills development, education–industry collaboration, and ecosystem building at the national and European level, while avoiding duplication of efforts and ensuring the efficient use of available resources.

Therefore, in consideration of the mutual interests above, the Parties agree on the following:

1. PURPOSE

The purpose of this MoU is to provide for a framework of cooperation and determine specific collaboration arrangements between the Parties as well as to establish a communication channel, intending to effectively cooperate in the matters of common interest, in particular in the field of cybersecurity skills and the CyberHubs project’s activities, based on the principle of common interest and complementarity.

Cooperation between the Parties encompasses, in particular but is not limited to, the following areas and activities whereby:



2. SCOPE

Cooperation between the Parties encompasses, in particular but is not limited to, the following areas and activities, whereby:

2.1. The Parties exchange information, data, and knowledge to identify synergies between their respective initiatives and projects in the areas of cybersecurity skills development, skills intelligence, workforce analysis, and professional education, training, upskilling, and reskilling.

2.2. The Parties may take part, as appropriate, in meetings, workshops, or events convened in the framework of their respective activities or relevant work strands, in matters where the other Party has an interest, expertise, or strategic relevance.

2.3. CyberHubs defines appropriate means and provides opportunities for the Associated Partner to contribute, on a voluntary and best-effort basis, to one or more CyberHubs activities or work areas, including but not limited to:

- national or European-level cybersecurity skills analysis and strategy development,
- education–industry cooperation initiatives,
- community-building and awareness-raising actions,
- knowledge-sharing and peer-learning activities within the CyberHubs network.

2.4. The Associated Partner supports the objectives of the CyberHubs project by promoting relevant CyberHubs outputs, results, and activities within its own stakeholder networks, with particular attention to national, regional, or sectoral contexts, through self-defined communication and dissemination actions.

2.5. The Associated Partner may co-organise and/or participate in CyberHubs events and initiatives during and, where relevant, beyond the project lifetime, including conferences, workshops, hackathons, training activities, or public-facing events aimed at engaging local and European cybersecurity skills ecosystems.

2.6. CyberHubs grants the Associated Partner visibility through appropriate communication channels, such as inclusion on the CyberHubs website, acknowledgement in dissemination materials, and participation in joint communication activities, subject to mutual agreement and branding guidelines.

2.7. CyberHubs may provide communication materials, guidelines, or toolkits to support the Associated Partner's dissemination of CyberHubs-related activities and results, where relevant and available.

3. INTENTION TO COLLABORATE

3.1. This MoU is a statement of intent and does not create any enforceable rights or obligations. The Parties will fulfil their commitments under this MoU on a best-efforts basis, except where limited by either Party's statutes, internal regulations, consortium agreements, or any other governing agreements.

3.2. This MoU does not restrict any of the Parties' independence and management of any project originating from its organisation, nor restricts the possibility of the development of any other cooperation or joint project of mutual interest.



3.3. Unless expressly set forth in this MoU, the Parties do not have the authority to act on behalf of, be liable for the acts of, or bind the other Party in any way. Neither Party shall enter into any contract or commitment on behalf of the other Party.

3.4. Nothing in this MoU shall create any employer/employee, agency, distributor, or any form of joint venture relationship between the Parties.

3.5. There will be no third-party beneficiaries to this MoU.

4. IMPLEMENTATION

4.1. This MoU will be implemented by mutual agreement and regular consultation between the Parties.

4.2. Further aspects of the cooperation between the Parties as the detailed working methods and procedures may be developed and agreed upon within the framework of the present MoU.

5. CONFIDENTIALITY

5.1. The Parties agree not to disclose to third parties any confidential information shared by the other Party in the context of this MoU. This Article survives the termination and expiration of this MoU, whatever the reason thereof.

5.2. If interest is expressed by either of the Parties, the Parties could, but are not obliged to, agree to convene a bilateral meeting to review the progress of the activities, and exchange relevant information about their activities, or plan future activities.

5.3. The Parties may collect and store personal data in connection with the present MoU and shall respect the provisions of the General Data Protection Regulation (EU) 2016/679 without using the personal data received from another Party for any other matter than performing the present MoU.

5.4. In case of any other specific restrictions related to the use of personal data, the providing Party shall inform the receiving Party about such restrictions of use.

6. BRANDING

6.1. Neither Party shall use the name, emblem, or trademarks of the other Party, nor any of its subsidiaries, and/or affiliates, nor any abbreviations thereof, outside the scope of this MoU, without the written approval of the other Party in each case.

6.2. The Parties agree to be publicly named as members of this MoU.

6.3. Whenever relevant, the Parties agree to use each other's logo and adhere to branding and marketing guidelines regarding their use in all communications related to this MoU.

7. APPLICABILITY, AMENDMENT, AND TERMINATION

7.1. This MoU shall enter into effect on the date of signature by the last Party.

7.2. This MoU may be amended by mutual written consent of the Parties.



7.3. Either Party may terminate this MoU by providing two (2) weeks' written notice to the other Party.

For the CyberHubs Project

For the CyberHubs Associated Partner

Signature: _____

Signature: _____

Name:

Name:

Date:

Date:

Place:

Place:

Disclaimer: All the activities linked to the management of the CyberHubs project are performed by project consortium partners in accordance with the grant agreement, and no additional compensation (fees) is linked to these activities.



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.