European Cyber Security Organisation ASBL
Rue Ducale 29 B – 1000 Brussels, Belgium
Web: www.ecs-org.eu Contact point: luigi.rebuffi@ecs-org.eu

European Cyber Security Organisation ASBL

2022 Membership Application Form

(All fields marked with * are mandatory for acceptance of the request)

Thank you for your interest in becoming a Member of ECSO ASBL. Please proceed by completing this *Membership Application Form*.

A prerequisite to answer some of the questions below and to become a Member is to read and accept the Statutes of our organisation. Operational details are described in our organisation's Bylaws. You may find these 2 documents on the ECSO official website (www.ecs-org.eu).

Please send the filled in and duly signed (end of the document) Membership Application Form to luigi.rebuffi@ecs-org.eu .

Further to your membership submission, it may happen that we request additional information from you, on behalf of the Association, to allow the ECSO Board of Directors to better consider your application and decide regarding your membership.

To be admitted as an ECSO Member, you must be:

(a) a Legal Entity established in at least one ECSO Country[1], or

(b) a public body from an ECSO Country.

MEMBERSHIP FEES (see also Annex I for rules on Membership Fees)

Each ECSO member is due to pay a membership fee. This is important as only with sufficient resources can we provide adequate and quality support to reach the objectives identified by the ECSO Association.

The calculation of these fees is based on your organisation's category, the turnover or budget, according to usual approaches.

For **2022**, the full year membership fees will be as specified in the table below.

Application as: *(Please tick one answer only*)*

ECSO Categories	**Annual fee €**	
Large providers (directly represented) of cybersecurity solutions / services providers	13200	☐
SMEs (as per E. Commission definition[1]) solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators - medium sized	4400	☐
SMEs (as per E. Commission definition[1]) solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators - small sized	2200	☐
SMEs (as per E. Commission definition[1]) solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators - micro sized	1100	☐
Research organisations (directly represented) with 250 employees or more	6600	☐

[1] An ECSO Country is defined as:

(a) a Member State of the European Union (a Member State) or an EEA / EFTA country, or UK

(b) a country associated to the EC Horizon Europe Programme

Universities, Academies or Research organisations (directly represented) with less than 250 employees and more than 50 employees; Associations composed only by Research Centers, Academies or Universities	2200	☐
Research organisations with less than 50 employees; Associations composed only by Research Centers, Academies or Universities	1100	☐
EU and National / Local Associations / Organisations / Clusters representing interests at national or European / International level (organisation budget > €1 mln)	6600	☐
EU and National / Local Associations / Organisations / Clusters (organisation budget > €500k and < €1 mln)	4400	☐
EU and National / Local Associations / Organisations / Clusters (organisation budget < €500k)	2200	☐
EU and National / Local Associations / Organisation / Clusters of Users	1650	☐
Users / Operators (not providing cybersecurity services) with 250 employees or more	2200	☐
Users / Operators (not providing cybersecurity services) with less 250 employees	1100	☐
Financial bodies (investors, insurances, …)	2200	☐
National Public Administrations	0	☐
Sub-national Administrations (e.g.: region, länder, province, town, etc.)	2200	☐

[1] NOTE ON SMEs

Staff headcount		Turnover	or	Balance sheet total	
< 250		≤ € 50 m		≤ € 43 m	
< 50		≤ € 10 m		≤ € 10 m	
< 10		≤ € 2 m		≤ € 2 m	

A) DETAILS OF THE ORGANISATION APPLYING FOR MEMBERSHIP

Full Name of the Organisation*:

Short Name of the Organisation:

Postal Address: Street Name or P.O.Box*:

Postal Address: Number*:

Postal Address: Town*:

Postal Code / Cedex*:

Country*:

Internet Homepage:

If your organisation/company belongs to a larger group or is an affiliated company, please give the name of affiliated organisation/company:

VAT Number*:

Billing address

If it is different from the postal address above, please add it here:

Street Name or P.O.Box: Number:

Town: Postal Code / Cedex: Country:

ORGANISATION PROFILE*: (Short general description of your organisation, at least 5 lines of text)

CYBERSECURITY RELATED ACTIVITIES*: (More specifics on cybersecurity related activities of your organisation, at least 5 lines of text)

COMPLIANCE WITH ECSO BYLAWS*: Please specify how you comply with ECSO Bylaws Art 3.2.2: "*The legal entity should have, either itself or through its sister companies,* ***R&D and manufacturing or service providing activities in an ECSO Country with significant European added value*** *and be able to demonstrate to the satisfaction of the Board of Directors that they* ***have a genuine business interest in the development of the European cybersecurity market***".

INTEREST IN PARTICIPATION IN ECSO WORKING GROUPS

Please express hereafter your interest in participating to the ECSO WGs activities (see short description in the Annex II, at the end of this document)*

WG1: Standardisation, certification and supply chain management ☐

WG2: Market deployment, investments and international collaboration ☐

WG3: Cyber Resilience of Economy, Infrastructure and Services (CREIS) ☐
- CSC – CISOs Strategic Committee ☐
- CEC – CISOs European Community ☐
- CoV – Community of Verticals ☐

Covered verticals (as per the definition given by the NIS Directive and subsequent revised NIS 2)

Healthcare	☐
Energy	☐
Finance	☐
Transport	☐
Smart citizens/smart working/smart environments	☐
Manufacturing (industry 4.0, …)	☐
Utilities, food, water	☐
eGovernment	☐
Telecom, media, and content	☐
Retail, eCommerce, eServices	☐

WG4: Support to SMEs, coordination with countries and regions ☐

WG5: Education, training, awareness, cyber ranges, human factors
☐

European Human Resources Network for Cyber (EHR4CYBER) Task Force ☐
Women4Cyber ☐
Youth4Cyber ☐
Cyber Ranges ☐
Education & Professional Training ☐

WG6: Strategic Research and Innovation Agenda (SRIA) and cybersecurity technologies ☐

B) MAIN CONTACT POINT AND REPRESENTATIVE OF THE MEMBER ORGANISATION

Family name*

First name(s)*

Title

Gender* ☐ Male ☐ Female

Position in organisation*

Department / Faculty / Institute / Laboratory / Group name

Phone*

Email*

ADDRESS OF THE MAIN CONTACT POINT (IF OTHER THAN A)

Street name Number

Town

Postal code / Cedex Country

COMPLIANCE WITH GDPR

ECSO is GDPR compliant and is following a transparent policy (https://ecs-org.eu/documents/data-privacy-policy.pdf).

Allowing ECSO to implement correctly GDPR is a shared responsibility between the secretariat and members. In becoming ECSO member, each organisation commits to inform the ECSO secretariat in changes of individual contacts that could potentially cause breaches in security or GDPR implementation. For instance, members should inform and request the ECSO secretariat to remove a person from a mailing list and delete its access to the portal once this person does no longer work for the company or changes departments that are not following the work of ECSO.

The information you provide in this form will be used solely for dealing with you as a member of ECSO.

ECSO has a Data Privacy Policy which can be found at https://ecsoportal.ecs-org.eu . Your data will be stored and used in accordance with this Policy.

If you/ the individuals listed above later wish to withdraw consent, please contact secretariat@ecs-org.eu.

I confirm that I am authorised to formally represent my company/organisation or subgroup thereof, and have read and agree with the ECSO ASBL Statutes and Bylaws (for the period of "provisional membership", explained in this membership form, I agree on the mentioned confidentiality of received information).

Date*:

Signature of authorised representative*: _____

ANNEX I: RULES ON MEMBERSHIP FEES

ECSO membership fees should be paid within 6 months of the invoice issue date. Only members that have paid their fees are granted the right to vote and be elected during the General Assembly at the Board of Directors and/or at Working Groups level. In case of non-payment of the membership fees within 6 months from the issue date of the invoice, the ECSO secretariat will send, before that deadline, 2 warning letters. If, after this period and the two warning letters, the fees have still not been paid, membership will be suspended by a decision of the ECSO Board of Directors. If no regularisation action of the payment of fees is undertaken following the suspension by the Board, membership will be automatically terminated at the following ECSO General Assembly. In case a member has not paid fees and has not announced on time its desire to end membership[2], a fee collection company will be mandated to collect the due fees amount.

Subsequent to the decision of the ECSO Board of Directors, your membership candidacy must be sponsored by a current ECSO member of the Board of Directors (see ANNEX III). The "sponsoring" implies that the Board Member knows sufficiently well your organisation and is ready to answer on your behalf to potential questions from other Board members to support your contribution to ECSO, its objectives and its values. If needed, the ECSO Secretariat will establish a link between you and a member of the Board to establish such "sponsoring" relationship.

Subsequent to the decision of the ECSO Board of Directors, membership fees will have a quarterly decrease during the year based on the period of the official membership approval:

- January-March: Full membership fee
- April-June: 75% of the membership fee
- July-September: 50% of the membership fee
- October-December: 25% of the membership fee.

Ahead of the formal membership approval by the full ECSO Board of Directors, "provisional membership" can be provided soon after your membership request has been sent to the ECSO Secretariat. In this case, you will be allowed to participate in ECSO activities (Working Groups, events, etc.) yet without voting rights and the possibility of being elected. These rights will be granted to you once the ECSO Board of Directors approves the full membership – the Board of Directors gathers 4 times a year.

During the "provisional membership period", provisional members will already receive all information provided to approved ECSO members. The information and documents the "provisional member" will get access to prior to the formal approval of its Membership should be considered as confidential. It is therefore forbidden to forward or share the information or documents to any other body without the formal consent of the ECSO Board.

[2] Each member has to notify the ECSO Secretariat by the end of September of the ongoing year at the latest, the membership termination becoming effective during the ECSO General Assembly of the following year.

ANNEX II: ECSO WG DESCRIPTION

WG1: Standardisation, certification and supply chain management

- Mission:
  - Support the roll-out of EU ICT security certification schemes, standard and legislation recommendations (MoU with ETSI, CEN/CENELEC, collaboration with EC, ENISA and JRC, member of the SCCG) and the establishment of trusted supply chains.

- Objectives
  - Understand the challenges of the industry in using standards and certification schemes.
  - Understand the needs of the market to identify the gaps in standardisation and propose a roadmap for priorities.
  - Define methodologies and approaches to facilitate and support the use of certification schemes.
  - Address the challenges for a trusted supply chain and management of the risks.
  - Study and explain system and service lifecycle and associated risk management.
  - Provide guidelines & recommendations on European legislations and policy initiatives.
  - Cooperation with EU bodies: ENISA, EC, European SDOs and other relevant stakeholders

- Segmentation
  - Sub WG1.1: Connected Components
  - Sub WG1.2: Digital Services and systems

WG2: Market deployment, investments and international collaboration

- Mission
  - Reduce the fragmentation of the European cybersecurity market and create sustainable strategies and tools to boost the level of investment in European cybersecurity industry.

- Objectives
  - Analyse and provide insights on the European cybersecurity market and support ECSO members to improve their market knowledge and current trends.
  - Provide access-to-finance and access-to-market opportunities to the European cybersecurity companies.
  - Create a forum for investors, policy-makers and supporting industries to discuss the EU cybersecurity market investment strategies and investigate new business opportunities inside and outside Europe.

- Segmentation
  - SWG 2.1 Market knowledge
  - SWG 2.2 Investments and innovative business models
  - SWG 2.3 International cooperation, global competitiveness and support to export

WG3: Cyber Resilience of Economy, Infrastructure and Services (CREIS)

- Mission and objectives
  - ECSO wants to engage directly with users (operators, companies, governments) to establish a true cybersecurity ecosystem, linking supply and demand and act as a transversal Working Group that defines needs of the sectors for standardisation / certification, education, training and exercises, research / technologies and local / regional impact.

- Segmentation

CREIS is structured as a three-level pyramid.

- At the bottom, there is the Community of Verticals (CoV).
- In the middle the CISOs European Community (CEC).
- At the top level features the CISOs Strategic Committee (CSC).

In the different levels of the pyramid the Traffic Light Protocol (TLP) is applied according to the discussions specific to that level as the confidentiality setting by default – red for the CSC, amber for the CEC, green for the CoV.

CSC – CISOs Strategic Committee (red level)

Trusted Cooperation and strategic intelligence sharing among CISOs of essential and important entities.

The CSC aims to allow CISOs from essential and important entities (using the working of the NIS2) to have a confidential and trusted exchange of strategic intelligence among themselves and establish links with CSIRTs and law enforcement authorities. Membership is open to ECSO members' CISOs only, and to non-ECSO members while they finalise their ECSO membership procedure.

Main objectives of the CSC:

- IOCs (Indicator of Compromise) pan-European platform
- Supply chain – Enhanced security related contractual engagements
- Strategic Threat Intelligence and Information sharing among Users & Operators.
- Platform / network to support Rapid Reactions of private operators: umbrella to support private sector in case of crisis for operational cyber resilience.
- Risk Management & Threat Information Coordination - red level
- Cooperation with the EU network of CSIRTs

CEC – CISOs European Community (amber level)

Policy support to CISOs and general information sharing

The CEC aims to allow CISOs from all companies and EU countries to exchange lessons learned and best practices, share information on operational issues, develop positions and/or link with the ISACs and the European institutions, through regular networking and meetings on specific issues. Membership is open for free to ECSO members' CISOs, but also to non-ECSO members CISOs on an ad personam level although non-ECSO members' CISOs will have limited/restricted rights and an annual participation with a limited fee.

Main objectives of the CEC:

- Interaction with EU Institutions on policy and legislative priorities (e.g. NIS 2)
- Link with EC initiatives, incl. Joint Cyber Unit for NIS 2 and NIS Coordination Group
- Networking of CISOs across sectors and countries
- Risk Management & Threat Information Coordination - amber level
- Cooperation with / development of efficient and trusted ISACs at EU level
- Other operational or policy initiatives from CISOs needs

CoV – Community of Verticals (green level)

Policy support and networking for the different vertical applications

The CoV is intended to be an open forum of exchange to facilitate the dialogue between Users (operators, companies, governments) and Suppliers/Providers of cybersecurity solutions to understand cyber threats and needs, envisage possible solutions, and support implementation of trusted and resilient solutions for key "verticals". Membership is open to any representatives from ECSO members, but also to non-ECSO members that are part of a stakeholders' list.

Main objectives of the CoV:

- Link with EC activities (e.g., certification – ECSO WG1 & legislative issues) – green level
- Users' strategic needs for sovereign solutions
- Federate European SOCs providers and Users
- Support NIS-D implementation

- Other policy or legislative aspects stemming from the users / suppliers interaction

WG4: Support to SMEs, coordination with countries and regions

➢ Mission
- Increase visibility of the European cybersecurity start-ups and SMEs outside their traditional home markets, support the inter-regional cooperation and the implementation of the regional smart commercialisation strategies.

➢ Objectives
- Promote Europe-based cybersecurity provider, their products and services.
- Facilitate cooperation among Europe's regional authorities and EU policy makers to exchange good practices and improve the competitiveness of local cybersecurity start-ups and SMEs.
- Stimulate a pan-European network of sales to develop the marketing skills of the local cybersecurity start-ups and SMEs and to accelerate their competitiveness at the European level.
- Raise awareness of the need to improve and deploy cybersecurity solutions for SMEs as users.

➢ Segmentation
  - SWG4.1: SMEs, start-ups and high growth companies
  - SWG4.2: Coordination of national and regional activities
  - SWG4.3: Support to Central and Eastern European Countries

WG5: Education, training, awareness, exercises

➢ Mission
- Contribute towards a cybersecurity capability and capacity-building effort for a cyber resilient next generation (NextGen) digital Europe, through increased education, professional training, skills development, as well as actions on awareness-raising, expertise-building and gender inclusiveness.

➢ Objectives
- Education & skills: Skills verification, minimum curricula and industry cooperation (universities), Youth4Cyber (education modules ages 6-26), including the most appropriate tools and learning methods to develop applicable capability, such as cyber ranges.
- Training/operational competences: EHR4CYBER (HR/jobs), building up a cybersecurity training and exercise ecosystem, as well as a European Cyber Range Community.
- Awareness/cyber hygiene/gender inclusiveness: Women4Cyber Foundation's national chapters, role model campaigns, etc., collaboration on awareness campaigns with EU institutions/Agencies; etc.
- Human factors: Link with citizens and civil society on aspects related to ethics, privacy, awareness, fight against cyber-crime, and societal impact.

➢ Segmentation
  - SWG5.1: Cyber Range environments and technical exercises
  - SWG5.2: Education and professional training
  - European Human Resources Network for Cyber (EHR4CYBER) Task Force
  - Women4Cyber
  - Youth4Cyber

WG6: Strategic Research and Innovation Agenda (SRIA) and cybersecurity technologies

➢ Mission:
- Define the cyber security EU R&I roadmap and vision to strengthen and build a resilient EU ecosystem. Analyse the challenges of digitalisation of the society and industrial sectors to sustain EU digital autonomy by developing and fostering trusted technologies.

- Objectives
  - Pursue the Strategic Research and Innovation Roadmap and vision to strengthen the European cybersecurity ecosystem.
  - Monitor the future Horizon Europe and Digital Europe Programmes and investment opportunities for R&I.
  - Coordinate the cybersecurity activities across cPPPs, CCN Pilots and other EU Initiatives: analysis of roadmaps
  - Provide inputs to relevant cyber security technologies for dual use technologies
  - Support the activities of the European Commission for the implementation of the R&I programmes
  - Work in coordination with JRC on taxonomy from Research to Market (mapping of taxonomies)

- Segmentation
  - SWG6.1: Ecosystem
  - SWG6.2: Digital Transformation in Verticals
  - SWG6.3: Data & Economy
  - SWG6.4: Basic & Disruptive Technologies
  - SWG6.5 Cybersecurity for dual use technologies

ANNEX III: PROVISIONAL MEMBERSHIP AND SPONSORING FROM A BOARD MEMBER

1) Candidate memberships will be submitted to the provisional approval of the "Provisional Membership Committee" of ECSO. At this stage, members of this committee will be given the opportunity to provide sponsorship to the candidate member on behalf of their respective company / organisation.
   a. If the provisional membership as well as a sponsorship are granted by the Chair and Vice Chairs of the ECSO Board of Directors, the provisional membership will be officially presented to the next Board of Directors meeting for formal approval.
   b. If the provisional membership is granted by the Chair and Vice Chairs of the ECSO Board of Directors but no member of the Provisional Membership Committee is proposing itself as "sponsor", the ECSO Secretariat will impartially and transparently facilitate the contact between the Point of Contact of the provisional member and suitable ECSO Directors[3] (1) for sponsoring purposes. If a sponsoring is not granted before the next Board of Directors meeting, the provisional membership will be submitted to a formal decision to the Board of Directors.
   c. If no provisional membership and no sponsoring are granted to a candidate member before the Board of Directors meeting, the candidacy will be directly submitted at the Board of Directors for formal decision, also to possibly find a "sponsor" among the Board members.

[3] suitable ECSO Directors: a suitable ECSO Director in this context means a company or organisation elected by the General Assembly as member of the ECSO Board of Directors and which operates in the same / similar sector as the candidate member or originate from the same / close ECSO Country or that for any other reason could be interested in the candidate member.

2) All membership requests should be sent to the ECSO Secretariat no later than 1 week before the Board of Directors meeting. Should the Secretariat receive a membership request after this deadline, the candidate will therefore not be granted provisional membership and its candidacy will directly be submitted to the Board of Directors for formal decision. In the meantime, the Secretariat will impartially and transparently facilitate the contact between the Point of Contact of the provisional member and a suitable ECSO Directors for sponsoring purposes.

As a reminder, the provisional members will be allowed to participate in ECSO activities (Working Groups, events, etc.) yet without voting rights and the possibility of being elected. These rights will be granted to you once the ECSO Board of Directors approves the full membership – the Board of Directors gathers 4 times a year.

During the "provisional membership period", provisional members will already receive all information provided to approved ECSO members. The information and documents the "provisional member" will get access to prior to the formal approval of its Membership should be considered as confidential. It is therefore forbidden to forward or share the information or documents to any other body without the formal consent of the ECSO Board.