European Cyber Security Organisation ASBL
2024 Membership Application Form (ANNEXES)

ANNEX I: RULES ON ECSO MEMBERSHIP FEES

ECSO membership fees shall be paid within 60 days of the invoice issue date (in any case, before the date of the Annual General Assembly of June).

Only Members having paid the ECSO fees are granted the right to vote and be elected during the ECSO General Assembly at the Board of Directors and/or at Working Groups level.

In case of non-payment of the ECSO membership fees within 60 days from the issue date of the invoice, the ECSO secretariat will send 2 warning letters. If, after this period and the two warning letters, the fees have still not been paid, the ECSO membership could be suspended by a decision of the ECSO Board of Directors and a penalty could be applied.

If no regularisation action of the payment of fees is undertaken following the suspension by the Board, membership will be terminated at the following ECSO General Assembly.

In case an ECSO Member has not paid fees and has not announced on time its desire to end its membership[1], 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.

TERMINATION OF ECSO MEMBERSHIP

Each member shall 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

EU Legal and Policy Task Force

The EU Legal and Policy Task Force is meeting remotely every month on remote connection to provide an update on EU policies activities and other cybersecurity initiatives in Brussels gathering contributions from ECSO Members.

- Mission:
  - Provide political intelligence to ECSO members by gathering information and drafting actionable briefings for ECSO Members to anticipate key developments in European cybersecurity legislation.
  - Support to all ECSO Working Groups by analysing both horizontal and vertical European cybersecurity legislation.
  - Improve cybersecurity policies in Europe by engaging with EU policy makers to help them draft cybersecurity policies that work for the European cybersecurity ecosystem.

- Ongoing work:
  - Monitoring policies of both vertical and horizontal EU cybersecurity legislation, including the Cyber Resilience Act, NIS2, AI Act, DORA, Cybersecurity of EUIBAs, and the certification schemes of the EU Cybersecurity Act.
  - Participating in public consultations and hearings on the Cyber Resilience Act with the European Parliament, Council and European Commission.

WG Trusted Supply Chains

- Mission:
  - Support the development and establishment of trusted supply chains by proposing methodologies and approaches for the management of the risks of products and services, including understanding the technical implication of legislations and regulations, and supporting the roll-out of cybersecurity certification schemes (MoU with ETSI, CEN/CENELEC, collaboration with EC, ENISA and JRC, member of the SCCG).

- 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 certification.
  - 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

WG Investments & Market Development

- 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.
  - 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.
  - 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.

WG Cyber Threat Management

- Mission and objectives of the CISO Network
  - Create a trusted environment for practitioners and end-users in cybersecurity where they can share information, lessons learned and best practices to increase cyber resilience of European companies and organisations.
  - The CISO Community leverages upon two channels in Signal to exchange news on cyber threats and another to comment and exchange best practices. The Traffic Light Protocol (TLP) is applied when needed.
  - The CISO Community meets once per month remotely and once per year at the flagship physical event "CISO Meetup". Other physical or remote meetings are organised periodically on specific issues

- Mission of the SOC/CTI Task Force:
  - Open the discussion among private European stakeholders develop and convey common messages and suggestions / recommendations to the EU and national decision makers for possible future public / private cooperation in the CTI domain.
  - Create the basis and possibly an ambiance for an increased and more efficient exchange of threat information among private stakeholders.

Ongoing work:

- The Task Force will continue common discussions on next steps on SOCs and the possibility to set up a European CTI approach and Platform.
- Meetings of the SOC / CTI TF are manly foreseen on remote connection to define objectives, incentives and models for the development of a European Cybersecurity Threat Intelligence Alliance.

.

WG Skills & Human Factors – Road2Cyber

- 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

- Cyber ranges / training / operational competences: gathering cyber range providers and end users, showcasing the European cyber range ecosystem and supporting the uptake of cyber ranges and cyber range-enabled services.
- Education: Minimum curricula guidelines for cybersecurity courses for university, higher education and professional training providers, and industry-academia collaboration.
- Skills/HR: Support to HR, skills verification and mapping to training and career paths, contribution to ENISA's European Cybersecurity Skills Framework (ECSF), development of the European HR Community, launch of a dedicated European cybersecurity job platform.
- Awareness/cyber hygiene/gender diversity/human factors: Youth4Cyber, Women4Cyber, awareness calendar, collaboration on awareness campaigns with EU institutions/Agencies, etc., and link with citizens.

WG Technologies & Innovation and Defence + Space

➢ 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)

ANNEX III: ECSO PROVISIONAL MEMBERSHIP AND SPONSORING FROM A BOARD MEMBER

1) Candidate memberships will be submitted to the provisional approval of the ECSO "Provisional Membership Committee". 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[2] (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 ECSO 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.

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 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] 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.

ANNEX IV: ECSO MEMBERSHIP PERIMETER

ECSO membership perimeter approved by the ECSO Board of June 29 2021 (rule applied but not yet introduced in the Statutes – waiting for the implementation of the "Community" following the ECCC Regulation)

- Full Members (all usual rights and obligations): Any public or private stakeholder member of the Community (ECCC) having a legal status and having their main HQ in in European Union, EFTA countries or UK. Access to and vote in GA, Board and Chairs. Access to all ECSO activities (Committees, WGs, TFs and "Editorial teams") and information.

- Associated Members: Any public or private stakeholder member of the Community (following ECCC/NCCs decision) with main HQ not in EU, EFTA countries or UK. Access to and vote at the GA (no vote for Board election), no access to Board, WG Chairs or Committees. Access to WGs and TFs with exception to "WGs / subWGs or other ECSO bodies dealing with sensitive issues", access to Editorial teams (when they are not a unique participant), access to specific non sensitive initiatives and information.

- External Members: Any public or private stakeholder non-member of the Community (for whatever reason) having a legal status in countries having access to EC programmes (HEP and DEP). No access to GA, Board, Chairs or Committees. Access to WGs, TFs and information as allowed by specific Board decision.

- Partners: Any public or private stakeholder member of the Community not demanding formal membership (no ECSO member): They participate in the Community activities at national or EU level promoted by NCC or the ECCC and could participate in some specific ECSO initiatives following payment of a "ticket". Access only to non-sensitive information in case of WGs and TFs policy topics.

- Institutional Partners: Other public stakeholders invited by the Board or WG/TF Chairs to our events / meetings (e.g. EP, EC, ENISA, …).

Reminder: definition of Community according to the REGULATION (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Art 8.2: The Community shall consist of industry, including SMEs, academic and research organisations, other relevant civil society associations as well as, as appropriate, relevant European Standardisation Organisations, public entities and other entities dealing with cybersecurity operational and technical matters and, where relevant, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges. The Community shall bring together the main stakeholders with regard to cybersecurity technological, industrial, academic and research capacities in the Union. It shall involve national coordination centres, European Digital Innovation Hubs, where relevant, as well as Union institutions, bodies, offices and agencies with relevant expertise, such as ENISA .

(interpretation of National Competence Communities deduced from the Regulation) Art 8.3: "Only entities which are established within the Member States shall be registered as members of the Community. They shall demonstrate that they are able to contribute to the mission and shall have cybersecurity expertise with regard to at least one of the following domains: (a) academia, research or innovation; (b) industrial or product development; (c) training and education; (d) information security or incident response operations; (e) ethics; (f) formal and technical standardisation and specifications."