

**DECISION No GB/2022/7**  
**of the European Cybersecurity Industrial, Technology and Research Competence Centre**  
**Governing Board**  
**on the Community membership and registration guidelines**

THE GOVERNING BOARD,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres ('ECCC')<sup>1</sup>, in particular Article 13 (3) (i),

Having regard to the rules of procedure of the ECCC and in particular Article 9-11 thereof,

Whereas,

- (1) According to paragraph 2) of Article 8 of the founding Regulation, 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.
- (2) Pursuant to point i) of paragraph 3) of Article 13 of the founding Regulation, the Governing Board shall take necessary strategic decisions, in particular with regard to the adoption of guidelines for assessing and registering entities as members of the Community.

HAS DECIDED AS FOLLOWS

Article 1

The document entitled 'Community membership and registration guidelines' annexed to this Decision is hereby adopted.

Article 2

This Decision shall take effect on the day following its adoption.

---

<sup>1</sup> OJ L 202, 8.6.2021, p. 1–31.

Done at Bucharest, on 23 June 2022

For the European Cybersecurity Industrial,  
Technology and Research Competence  
Centre

Pascal Steichen  
Chairperson of the Governing Board

***Annex:***

- ECCC and network of NCCs: Community membership and registration guidelines

# **ECCC and network of NCCs**

**Community membership and registration guidelines**



## I. Table of Contents

|  |           |
|--|-----------|
| <b>I. Table of Contents .....</b>  | <b>4</b>  |
| <b>1. Introduction.....</b>  | <b>6</b>  |
| 1.1. The legal basis for guidelines.....   | 6         |
| 1.2. The description of the ECCC .....   | 6         |
| 1.3. The role and tasks of the Community .....   | 7         |
| <b>2. Membership criteria / Membership requirements.....</b>                                       | <b>9</b>  |
| 2.1. Formal criteria.....  | 9         |
| 2.1.1. The type of entities.....   | 9         |
| 2.1.2. The cybersecurity expertise .....   | 9         |
| 2.1.3. The assessment on security grounds .....  | 10        |
| 2.1.4. Assessment on exclusion criteria on the basis of Article 136 of the EU Financial Regulation | 11        |
| 2.2. Contribution to the mission of the ECCC and the Network.....                                  | 11        |
| 2.3. Representatives of the entity .....   | 12        |
| <b>3. The application process .....</b>  | <b>13</b> |
| 3.1. The assessment of the Community membership applications .....                                 | 13        |
| 3.1.1. The assignment of applications.....   | 13        |
| 3.1.2. Ensuring balanced representation .....  | 14        |
| 3.2. Recommended timeline for assessment .....   | 14        |
| 3.3. The outcome of assessment and further steps.....  | 15        |
| 3.3.1. Acceptance – positive assessment.....   | 15        |
| 3.3.2. Rejection – negative assessment .....   | 16        |
| <b>4. Registration of entities by the ECCC .....</b>   | <b>17</b> |
| 4.1. The procedure to register by the ECCC .....   | 17        |
| 4.2. The membership duration .....   | 17        |
| <b>5. The Community Membership Management .....</b>  | <b>17</b> |
| 5.1. The revoking of the registration.....   | 17        |
| 5.2. The withdrawal of membership by members.....  | 18        |
| 5.3. The changes of registration data.....   | 18        |
| <b>6. The coordination and cooperation between NCC .....</b>                                       | <b>18</b> |

|            |   |           |
|------------|---|-----------|
| 6.1.       | The Community Membership Directory.....   | 18        |
| <b>7.</b>  | <b>The registration of Union institutions, bodies, offices and agencies .....</b> | <b>19</b> |
| 7.1.       | The procedure for assessing by the ECCC.....                                      | 20        |
| 7.2.       | Revoking of the registration.....   | 20        |
| <b>8.</b>  | <b>The review clause .....</b>  | <b>20</b> |
| <b>9.</b>  | <b>Executive Summary .....</b>  | <b>21</b> |
| <b>10.</b> | <b>ANNEXES .....</b>  | <b>22</b> |
| 10.1.      | ANNEX 1 – Membership Registration Form .....                                      | 22        |
| 10.2.      | ANNEX 2 The template to inform about the positive assessment.....                 | 25        |
| 10.3.      | ANNEX 2 – The Flow chart of the registration process .....                        | 25        |
| 10.4.      | ANNEX 3 – Article 136 of the EU Financial Regulation.....                         | 26        |

## 1. Introduction

The European Cybersecurity Industrial, Technology and Research Competence Centre (the ECCC), the Network of National Coordination Centres (the Network) and the Cybersecurity Competence Community (the Community) form the new strategic framework of strengthening cybersecurity capabilities in the European Union.

Based on the Article 8.2 of the Regulation (EU) 2021/887<sup>2</sup> (the Regulation), 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 European Union.

### 1.1. The legal basis for guidelines

The guidelines are established in compliance with Article 13.3.i of the Regulation which enables the Governing Board of the ECCC to adopt guidelines for assessing and registering entities as the members of the Community.

This guidance aims to encourage alignment between the National Coordination Centres (the NCCs) in procedure of assessment and provide recommendations in order to support the smooth development of the Community. The guidance is not legally binding and is under regular review.

### 1.2. The description of the ECCC

The ECCC is the Union body with legal personality established in 2021 through the Regulation. The ECCC performs a dual role, undertakes tasks in the area of cybersecurity industry, technology and research as defined in the Regulation, as well as managing cybersecurity-related funding from several programmes, in particular the Horizon Europe and the Digital Europe Programme. The ECCC is the main EU's instrument to pull investments in cybersecurity research, technology and industrial development and to implement projects and initiatives together with the Network.

**The mission** of the ECCC and the Network is to help the EU to:

- 1) strengthen its leadership and strategic autonomy in the area of cybersecurity by retaining and developing the EU's research, academic, societal, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security, including the confidentiality, integrity and accessibility of data, in the Digital Single Market;

---

<sup>2</sup> Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (Official Journal of the EU 8.06.2021 L 202)

- 2) support EU's technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the EU; and
- 3) Increase the global competitiveness of the EU's cybersecurity industry and ensure high cybersecurity.

The **overall objective** of the ECCC is to promote research, innovation and deployment in the area of cybersecurity in order to fulfil the mission. **The specific objectives** entail:

- 1) enhancing cybersecurity capacities, capabilities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society, as appropriate;
- 2) promoting cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification of the security of digital products and services, in a manner that complements the efforts of other public entities;
- 3) Contributing to a strong European cybersecurity ecosystem that brings together all relevant stakeholders.

The specific objectives are to be implemented by the ECCC by:

- 1) establishing strategic recommendations for research, innovation and deployment in cybersecurity in accordance with Union law and setting out strategic priorities for the ECCC activities;
- 2) implementing actions under relevant Union funding programmes in accordance with the relevant work programmes and the Union legislative acts establishing those funding programmes;
- 3) fostering cooperation and coordination among the National Coordination Centres and with and within the Community; and
- 4) where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary to fulfil the tasks set out in Article 5 and in accordance with the respective work programmes set out in point (b) of Article 5(3).

The governance of the ECCC comprises of a Governing Board, an Executive Director and a Strategic Advisory Group.

### 1.3. The role and tasks of the Community

The Community contributes to the mission of the ECCC and the Network, enhances, shares and disseminates cybersecurity expertise across the EU.

The Regulation foresees that in the EU there is one Community, where entities from all 27 Member States can become members. Nevertheless, it is clear that there is a need for cooperation also at the national level. The NCCs should play a role as the Community gatekeepers, at the initial stage through the application assessment procedure and later on actively organizing and supporting the cooperation of national members of the Community.

The members of the Community, in accordance with Article 9 of the Regulation, have the following tasks:

- 1) support the ECCC in fulfilling its mission and objectives and, for that purpose, shall work closely with the ECCC and the National Coordination Centres;
- 2) where relevant, participate in formal or informal activities and in the working groups referred to in point (n) of Article 13(3) to carry out specific activities as provided by the annual work programme; and
- 3) where relevant, support the ECCC and the National Coordination Centres in promoting specific projects.

The Community, through its working groups and in particular through the Strategic Advisory Group, provides the Executive Director and the Governing Board with strategic advice on the agenda, the annual work programme and the multiannual work programme, in accordance with the rules of procedure of the Governing Board.

The Community brings together stakeholders that are able to contribute to the mission and have cybersecurity expertise in the technological, industrial, academic and research areas.

The Community shall consist of:

- 1) industry, including SMEs;
- 2) academic and research organisations;
- 3) other relevant civil society associations;
- 4) European Standardisation Organisations,;
- 5) public entities and other entities dealing with cybersecurity operational and technical matters;
- 6) where relevant, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges.

The Community involves:

- 1) National Coordination Centres;
- 2) where relevant European Digital Innovation Hubs;
- 3) Union institutions, bodies, offices and agencies with relevant expertise, such as ENISA.



## 2. Membership criteria / Membership requirements

### 2.1. Formal criteria

#### 2.1.1. The type of entities

Only entities established in the Member States<sup>3</sup> can be members of the Community.

Different forms of legal organisation are possible, under the condition that they are in line with the law of the Member State where the application is submitted.

The Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect<sup>4</sup>.

Individuals (natural persons) acting as ad-hoc experts can provide their expertise when needed and therefore participate on specific activities, but cannot be registered as members of the Community.

All types of entities can be members of the Community, including but not limited to:

- 1) public sector entities;
- 2) private sector entities;
- 3) associations, organizations and collective bodies;
- 4) non-profit organizations.

Entities not established in a Member State cannot apply to become part of the Community.

#### 2.1.2. The cybersecurity expertise

The Regulation stipulates in Article 8.3 that:

members of the Community shall have cybersecurity expertise with regard to at least one of the following domains:

- 1) academia, research or innovation;
- 2) industrial or product development;
- 3) training and education;
- 4) information security or incident response operations;
- 5) ethics;
- 6) formal and technical standardisation and specifications.

---

<sup>3</sup> EEA EFTA states (Iceland, Liechtenstein and Norway) are considered as Member States, when formal requirements according to Council Regulation (EC) No 2894/94 concerning arrangements for implementing the Agreement on the European Economic Area are fulfilled

<sup>4</sup> C-131/12 Google Spain and Mario Costeja Gonzalez 13 May 2014, C-230/14 Weltimmo 1 October 2014

The notion of expertise requires to demonstrate certain level of knowledge or skills. Therefore, an entity should be able to demonstrate that it has been active in one or more domains listed above.

In order to demonstrate the cybersecurity expertise, the requesting entity should indicate the type of domain where it is active, accompanied by a supporting description of concrete activities performed.

### **2.1.3. The assessment on security grounds**

The Regulation states in Article 8.4 that assessment shall also take into account any relevant national assessment on security grounds made by the national competent authorities. Such registrations shall not be limited in time but may be revoked by the Competence Centre at any time if the relevant NCC considers that the entity concerned no longer fulfils [...] on justified security grounds. Where membership in the Community is revoked on security grounds, the decision to revoke shall be proportional and reasoned.

The purpose of the Community is to be “as open and inclusive as possible, as closed as necessary”. Security grounds are therefore a limitation/restriction to access the Community and therefore implementation can be done in specific and well-defined situations and should be clearly stated. This limitation/restriction is assessed by the NCC on a case by case basis.

The Regulation refers to national assessment on security grounds, therefore it is up to the NCC that receives the application to identify all relevant factors and apply them to the application of the requesting entity. This should be done individually, taking into consideration the circumstances of the concrete case.

The decision for negative opinion/rejection on a security grounds is a sovereign decision of the NCC. Nevertheless to ensure alignment how this provision is implemented and avoid forum shopping, the NCCs should closely cooperate and exchange information. The scope of the information to be shared is to be defined by the NCC that received the application. Nevertheless when the application receives a negative assessment, such information should be without delay shared within the Network and the ECCC.

The term security grounds is not defined in the Regulation. During the process of assessment it might be useful to take into consideration the jurisprudence of the European Court of Justice regarding this issue. To give an example, following rulings and opinions might be useful.

In judgement of 23 November 2010 (C-145/09) the ECJ stated that as regards public security, the Court has held that this covers both a Member State’s internal and its external security (see, inter alia, Case C-273/97 *Sirdar* [1999] ECR I-7403, paragraph 17; Case C-285/98 *Kreil* [2000] ECR I-69, paragraph 17; Case C-423/98 *Albore* [2000] ECR I-5965, paragraph 18; and Case C-186/01 *Dory* [2003] ECR I-2479, paragraph 32). Moreover, it concluded that the Court has also held that a threat to the functioning of the institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security (see, inter alia, Case 72/83 *Campus Oil and Others* [1984] ECR 2727, paragraphs 34 and 35; Case C-70/94 *Werner* [1995] ECR I-3189, paragraph 27; *Albore*, paragraph 22; and Case C-398/98 *Commission v Greece* [2001] ECR I-7915, paragraph 29).

Public security must therefore be understood to include not only the security of the Member State and its institutions, but also all the measures designed to counteract serious threats to the values essential to the protection of its citizens (Opinion of Advocate General, **C-145/09**)

Based on the security grounds application can be rejected or revoked for the already registered members of the Community.

#### **2.1.4. Assessment on exclusion criteria on the basis of Article 136 of the EU Financial Regulation**

The Regulation foresees in Article 8.4 that registrations shall not be limited in time but may be revoked by the Competence Centre at any time if the relevant National Coordination Centre considers that the entity concerned no longer fulfils the criteria set out in paragraph 3 (membership criteria) of this Article or falls under Article 136 of the EU Financial Regulation, or on justified security grounds.

Art. 136 of the EU Financial Regulation and equivalent national law apply to entities requesting to become members of the Community. The entity must not be in an exclusion situation such as the ones mentioned in Article 136 of the Financial Regulation.

Should the entity fall into any of the conditions listed in Article 136 of the EU Financial Regulation (see Annex 3), its membership may be rejected or revoked immediately with no further assessment. The rejection takes place following the application process to become the Member of the Community. The revocation is foreseen for the entities already registered as the members of the Community.

The entity should declare, upon requesting registration as a member of the Community, that none of the exclusion conditions described in the Article 136 of the EU Financial Regulation apply to it.

The NCC should in principle rely on the declaration provided by the entity. A closer analysis is recommended if the NCC has a suspicion whether the declaration is reliable.

The applicant or member of the Community shall immediately inform in writing the NCC should any of the exclusion conditions foreseen in the Article 136 of the EU Financial Regulation apply.

It should be also required in the application process and further, that only the Legal Entity Appointed Representative under national law (commonly known as LEAR) is authorised to sign such a declaration.

The LEAR shall also submit to the NCC on a biennial basis a declaration that none of the conditions listed in the Article 136 of the EU Financial Regulation apply.

## **2.2. Contribution to the mission of the ECCC and the Network**

The Regulation states that the Community should:

- (recital 17) benefit from the experience and the broad representation of relevant stakeholders built through the PPP on cybersecurity, ECSO, from the lessons learnt from four pilot projects, and from the pilot project EU FOSSA (Free and Open Source Software Audits).
- (recital 19) seek the exchange of developments in cybersecurity, including in products and processes, in standards and in technical standards, with the international community
- (recital 30) Help advance and disseminate the latest cybersecurity products, services and processes

- (recital 31) adapt quickly and continuously to new developments in the context of -changing nature of cyber threats and cybersecurity,
- (recital 34) provide input to the activities of the Competence Centre, to the multiannual work programme and to the annual work programme, in particular through the Strategic Advisory Group.
- (recital 34) The Community should also benefit from the community-building activities of the Competence Centre and the Network
- (recital 43) publicise the fact that their respective activities are undertaken in the context of this Regulation
- (Art 34.2) ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information in a timely manner, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Conflicts of Interests.

In a broad sense, the Community must contribute and be aligned with the ECCCs and the NCCs mission; therefore, the requesting entity should describe upon applying for membership how it will support the ECCC and NCCs in fulfilling their mission and objectives.

In order to accept or deny a membership request, the NCC is advised to carry out an assessment of the contribution of the entity to ECCC and NCC's missions in order to decide whether it is sufficient to pass the assessment.

### **2.3. Representatives of the entity**

Regulation specifies:

- (Art 8.8) An entity registered as a member of the Community shall designate its representatives to ensure an efficient dialogue. Those representatives shall have expertise with regard to cybersecurity research, technology or industry.

In order to streamline the process of the registration it is advised that the entity designates the representative already in the registration form. An entity can designate one or more representatives, but it should state which representative is the main person to represent the entity. An entity should inform the ECCC and the NCC if the representatives have changed providing the necessary information to register new representatives.

### **3. The application process**

To apply for membership in the Community, it is recommended that applicants fill out the membership registration form provided in a digital format on the website of the ECCC. The form should be sent directly to the NCC responsible for the assessment.

The process of application and registration should be digital.

The application should include information on the entity that enables an assessment on whether it meets the membership requirements as defined in the Regulation. To streamline the application, during the application process, the entity should indicate the representative/s in the application.

The proposed scope of information to include in the registration form is presented in Annex 1.

The procedure to apply should be simple, transparent and not limited in time. Nevertheless, the ECCC and / or NCC may reserve that an assessment will be made during certain periods of time. The recommended timeline is at least every 3 months. Such reservation should be stipulated during the application process.

If needed the ECCC / the NCC may ask the entity for additional information or clarification of the application.

Information on the rules of the application process should be publicly available on the ECCC website, as well as the NCC websites.

The NCC may involve actors well positioned within the national ecosystem to assist with the assessment procedure.

#### **3.1. The assessment of the Community membership applications**

In accordance with Article 7.1.(I) of the Regulation, the NCCs have the task of assessing requests by entities established in the same Member State as the NCC to become part of the Community.

Therefore, an entity cannot be registered by the ECCC as the member of the Community without prior assessment made by the respective NCC.

##### **3.1.1. The assignment of applications**

The applications to become a member of the Community can only be processed by the NCC where the entity applying for membership is established.

The applications by Union institutions, bodies, offices or agencies applying for community membership are processed by the ECCC.

When the application received by the NCC does not provide all the necessary information enabling the assessment, the NCC may ask the entity to complete or clarify the application.

When on the basis of the information included in the registration form it is clear that the NCC that received the application is not the NCC where the entity is established, if possible, the application should be sent to the competent NCC and the entity should receive information that the application will be assessed by another NCC.

It is recommended, that the NCC checks if the application by the same entity had been submitted to other NCCs and whether the assessment is pending or there has been a negative assessment. The list of pending cases and applications that were negative assessed should be included in the register provided by the ECCC. The list of pending cases and applications that were negatively assessed will be made available only to the NCCs and the ECCC.

### **3.1.2. Ensuring balanced representation**

The NCCs are encouraged to reach out, through various means, to national stakeholders, with special attention to SMEs, and actively provide information on the Community and possibility and procedure to join the Community.

Through the Network the NCCs should exchange the best practices how to ensure a balanced representation.

The ECCC should also actively inform the public about the Community, including the procedure to join it, advantages of joining and expected contribution from entities.

## **3.2. Recommended timeline for assessment**

The Regulation does not impose any time limitation neither for registration nor for assessment. Consequently, those administrative processes could last as long as necessary according to the steps (possible corrections) required and resources available in the ECCC / the NCCs for this matter. The respective timelines may be established in the national law or arrangements.

It is recommended to keep the registration continuously open for potential members to start the process by submitting applications.

The NCC can decide to gather pending applications and assess them on specific timeframes, creating assessment windows on certain moments of the year. Therefore, the result of the assessments would be only available at those moments, for instance once per quarter.

The ECCC may also decide on registration windows for the positively assessed applications, nevertheless as the registration is a technical action the ECCC should seek for the shortest possible deadlines.

Communication actions can be synchronized to those assessments windows and publications in order to announce newly registered members of the Community. Also, in “call to action” campaigns to encourage potential members to be part of the Community.

### **3.3. The outcome of assessment and further steps**

Since the Regulation foresees that the ECCC only registers entities that have been assessed by an NCC, no other assessment or restrictions by the ECCC are expected. The NCC positive assessment result is binding for the ECCC, therefore the ECCC cannot refuse to register an entity whose application was positively assessed by an NCC.

The result of assessment by the NCC, including possible corrections requests, can be the following:

#### **3.3.1. Acceptance – positive assessment**

In this case, the NCC, without delay, sends the registration form together with information that the result of the assessment was positive to the ECCC with request to register the entity.

The NCC does not have to provide to the ECCC further reasoning on the grounds of the positive assessment. It should be enough to send the information that the assessment is positive. The recommended template for such information can be found in Annex 2.

The NCC should inform individually the requesting entity (by e-mail or other digital channel) about the positive result of the assessment and submission of the application to the ECCC. It should also provide information that registration will be done by the ECCC.

Once the entity has been positively assessed by the NCC and the information about positive assessment together with the application have been sent to the ECCC, the next step is the official registration issued by the ECCC, as described in section 4 Registration of entities by the ECCC.

Once the registration is done, the ECCC should inform individually the entity (by e-mail or other digital channel) and all the NCCs through digital platform.

The ECCC should provide a digital register of the Community members. The register should be public and available through the ECCC website as well as the NCCs websites. The register should provide a quick and user friendly tool to find entities, in particular broken down into the kind of entity and the country of establishment.

The information provided by an entity in the application which is needed for the registration process, will be shared with the ECCC.

The information provided by an entity during the registration process may be shared with other NCCs.

It is recommended that the following information about entity is publicly available through the register provided by the ECCC:

- 1) name;
- 2) country of establishment;
- 3) website;
- 4) type of organisation as foreseen in Article 8.3 of the Regulation;

5) fields of activity.

Furthermore and in parallel, it is also recommended to communicate the new memberships in the Community on the NCCs websites, and encourage the entity to use its own channels to make that membership visible. Entities and their representatives could also make visible their participation on Community's activities.

The ECCC may provide materials for uniform visual identification of the members of the Community.

### **3.3.2. Rejection – negative assessment**

If the conditions described in section 2 are not met, the NCC may give a negative assessment.

Before issuing a negative assessment, the NCC should aim to clarify possible misinterpretations or missing documents with the entity.

It is recommended that prior to final negative assessment, the NCC informs, through the Network, other NCCs about the possibility of issuing the negative assessment. The NCC may also request within the set timeline, recommended 2 weeks after receiving request for any information that might be relevant.

In case of a rejection, the result of a negative assessment should be duly justified describing the grounds that motivated the rejection. Where the negative assessment is done on the basis of security grounds, the NCC may decide not to reveal all the circumstances that are justifying the decision.

The information about negative assessment result with the reasoning should be sent to the applicant (formal writing or email), together with the information about the possible next steps to follow in accordance with national law.

The next steps possible for the entity upon receiving the negative assessment should be defined in accordance with the national law. The information about the possible next steps under national law should be provided to the entities. In the case of a negative assessment the application is not submitted to the ECCC. It is recommended that the NCC informs the ECCC and other NCC through the Network about the negative assessment.

The NCC should provide on its website the information regarding the next steps. In order to help other NCCs should they receive a new request of a previously rejected entity in a different Member State, the NCC should notify each rejection, following the instructions described in section [Coordination and Cooperation between NCCs] of this document.

Rejected applicants should have the possibility to re-submit a new membership request at any time when desired once their rejection conditions have changed and not sooner than 3 months after negative assessment.

The information about a resubmission of the application to become member of the Community should be reflected in the register mentioned in the section 3.3.1.



## **4. Registration of entities by the ECCC**

### **4.1. The procedure to register by the ECCC**

According to Article 8.4. of the Regulation, the ECCC shall register entities, at their request, as members of the Community after receiving an assessment made by the National Coordination Centre of the Member State in which those entities are established to confirm that those entities meet the criteria set out in Article 8.3 of the Regulation.

After the assessment is completed, the ECCC is informed about the result. The ECCC will acknowledge the outcome of the assessment and register all entities which passed the assessment process as members of the Community and list them as members of the Community on the ECCC website.

Once the registration is done, the ECCC should inform individually the entity (by e-mail or other digital channel) and all the NCCs through digital platform.

The list of the Community members should be updated on regular basis. The Competence Centre shall also inform the NCCs about the newly registered members of the Community.

### **4.2. The membership duration**

The registrations of the entities are not limited in time. However, the ECCC may revoke the membership at any time and provide relevant justification of the decision in writing to the member (see below section 5.1)

## **5. The Community Membership Management**

### **5.1. The revoking of the registration**

If the requirements for membership in the Community cease to apply according to the above-mentioned membership requirements, membership shall be revoked by the ECCC.

The procedure of revocation can be initiated at any moment by the NCC where the entity is established if it has the information justifying the start of the proceedings.

The entity should be informed about the initiation of the procedure and have the possibility to present its position.

Prior to the decision on the revocation of the membership by the ECCC an assessment should be done by the NCC which was providing the assessment at the time of the registration. If the place of establishment of an entity has changed, the NCC responsible for assessment should be the one of the place of establishment.

The NCC should provide the reasoning for its assessment.

It is recommended that the NCC that intends to seek revocation of a member via the ECCC informs other NCCs about this revocation before making the formal request to the ECCC. The other NCCs can provide additional substantial information within the 2 weeks after receiving information. After 2 weeks the NCC can send the formal request to the ECCC. The NCC is not bound in any way by such additional information.

The NCC should send the assessment to the ECCC. The ECCC on the basis of this assessment, should revoke the registration.

## **5.2. The withdrawal of membership by members**

Any entity that wishes to withdraw from the Community shall formally communicate its intention to the NCC where it is established. The NCC may wish to ascertain the reasons for the withdrawal of Community membership and should seek to confirm the entity's request before informing the ECCC to revoke Community membership.

The NCC should send the withdrawal letter to the ECCC. On the basis of such letter, the ECCC deletes the entity from the registry.

## **5.3. The changes of registration data**

The entity should inform the NCC about any changes of the data presented in the registration form. Such obligation should be included in the registration form. In particular changes to the representatives, exclusion conditions, contribution to the mission and legal establishment.

The changes of the information provided in the registration form should be submitted to the NCC by the entity using the template of the registration form. In such a case, except of the name, the entity should fill only the fields of the form where changes occurred.

The NCC assesses the changes and sends the form to the ECCC to reflect the changes in the register.

# **6. The coordination and cooperation between NCCs**

The NCCs shall act as points of contact at national level for the Community to support the ECCC in fulfilling its mission and objectives and are advised in particular to coordinate with the Community through the coordination of Community members in their Member States (Article 7.1.a of the Regulation). To that end, NCCs shall, where relevant, cooperate through the Network (Article 7.4 of the Regulation).

As potential Community members may operate and provide services across the Union, may be established in several Member States or may be linked with other potential Community members in other Member State (in particular in the form of subsidiaries or partner enterprises), the NCCs are advised to coordinate and cooperate through the Network to find a mutually aligned way in building up the Community.

## **6.1. The Community Membership Directory**

Each NCC and the ECCC should designate a person responsible for the cooperation in the registration process. The list of contact persons should be available for the NCCs and the ECCC and updated if there is any change.

To facilitate effective Community Membership and Registration Management, the ECCC and the NCC should use a common digital database/registry listing pending, accepted and rejected registration requests. This database shall form the backend of the online membership registration form.

It is recommended that the ECCC and the NCCs use this tool to assign pending registrations to the responsible NCC, or in the case of EU bodies and institutions to the ECCC.

The ECCC and the NCCs should also use this tool to communicate on and coordinate registrations of entities that operate in more than one Member State.

All NCCs should check whether an entity already applied in another NCC or whenever a new application is submitted.

There might be situations where an entity whose application for membership is rejected by the NCC of one Member State, makes an effort to apply for membership with the NCC of another Member State, notwithstanding requirements on establishment. This would contravene first assessment and decision to reject and could undermine the trust in the Community as a whole. In addition, there might be a situation where big corporate groups apply with their subsidiaries in several Member States.

In case an entity or where several subsidiaries of a corporate group operate simultaneously in several Member State, the respective NCCs are advised to engage in a close dialogue with each other to ensure a coherent assessment procedure, recognising that there can be circumstances where subsidiaries in different Member States may make diverse contributions to the mission and have various types of cybersecurity expertise.

With a view to achieve an overview on the various application processes which might take place simultaneously and to avoid that entities can play NCCs off against each other, the NCCs should share information on the pending applications as well as on the rejected applications as soon as possible.

The information should contain at least the name of the applicant, the Member State where it applied and the date of application and, where relevant, the rejection reason/s.

All NCCs as well as the ECCC should have access to digital tool supporting the assessment and registration process.

The NCCs should use the Network as a platform to discuss the challenges emerging in the process of assessment, exchange best practises and seek for advice. The ECCC should support such a cooperation.

## **7. The registration of Union institutions, bodies, offices and agencies**

Article 8.6 of the Regulation stipulates that the ECCC shall register relevant Union institutions, bodies, offices and agencies as members of the Community after carrying out an assessment to confirm that that Union institution, body, office or agency meets the criteria set out in Article 8.3 of the Regulation.

In line with Article 8.3 of the Regulation the Union institutions, bodies, offices and agencies have to demonstrate that they are able to contribute to the mission of the ECCC and must have cybersecurity expertise at least in one of the following domains:

- 1) academia;
- 2) research or innovation;
- 3) industrial or product development;
- 4) training and education;
- 5) information security or incident response operations;
- 6) ethics or;
- 7) formal and technical standardisation and specifications.

### 7.1. The procedure for assessing by the ECCC

The assessment of the applications by the Union institutions, bodies, offices and agencies is made by the ECCC.

After positive assessment the ECCC registers the Union institution, body, office or agency as a member of the Community.

The process for applying and registration should be digital.

The guidelines for the assessment and registration process for the entities presented above apply accordingly.

### 7.2. Revoking of the registration

As stated in Art. 8.6 of the Regulation the membership can be revoked by the ECCC at any time if it considers that the Union institution, body, office or agency no longer fulfils the criteria set out in Article 8.3 of the Regulation or falls under Article 136 of the EU Financial Regulation.

## 8. The review clause

At the request of the Governing Board, the Executive Director shall periodically review the functioning of these guidelines, and report to the Governing Board. The Executive Director shall take into account input from the Network on the experience gained. The Executive Director should also consult with the Community and Strategic Advisory Group. The report may be accompanied by, where necessary, the proposal for changing the guidelines.

The first review shall be conducted 18 months after the date of the adoption of these guidelines.

Any member of the Governing Board may propose changes to these guidelines whenever such a need for changes occurs. The proposal should have a reasoning. The Executive Director should give an opinion on the proposed changes.

## 9. Executive Summary

These guidelines have been prepared to assist National Coordination Centres (NCCs) in undertaking the assessment process for membership of the Community. They also provide guidance on the role of the ECCC as regards registration of positively assessed entities as members of the Community. This document fulfils the requirements of the Governing Board in enabling the adoption of guidelines under Article 13(3)(i) of Regulation (EU) 2021/887.

The guidelines describe the mission, objective, role and tasks of the Community. The requirements of entities as regards establishment, expertise and contribution to the mission of the ECCC are then set out. This is accompanied by exclusion criteria as set out in the EU Financial Regulation and information on security assessment.

The application process is then described, with a registration form template and flow chart of the process set out in the Annexes. This includes the option of reliance on the digital tools of the ECCC and information flows on the assessment outcomes.

The guidelines also include sections on registration by the ECCC and on management of Community membership. There is a strong emphasis on coordination between NCCs involving the ECCC in regard to applications to facilitate alignment and prevent abuse. This includes provision for a transparent directory of Community members on the ECCC's website as well as a backend facility for administrative coordination.

Finally, these guidelines have been developed to facilitate the prompt establishment of the Community.

The guidelines will be reviewed periodically by the Governing Board taking into consideration the experience and best practises in the Network and the ECCC gathered during the assessment and registration process.

## 10. ANNEXES

### 10.1. ANNEX 1 – Membership Registration Form

#### Your organisation

|  |                      |
|--|----------------------|
| Name   | <i>Short text</i>    |
| Address  | <i>Short text</i>    |
| Company/organization registration number   | <i>URL</i>           |
| Is this your organisation's main seat / headquarter? (is your organisation a subsidiary of an organisation?) | <i>Y/N</i>           |
| If not, please provide the name and address of the main seat / headquarter                                   | <i>Short text</i>    |
| Website  | <i>URL</i>           |
| Phone number   | <i>Phone nr.</i>     |
| Email  | <i>Email address</i> |
| Organisation type  | <i>Short text</i>    |
| Does your organization have subsidiaries in other EU Member States (including EEA/EFTA countries)            | <i>Y/N</i>           |
| If yes, please specify   | <i>Short text</i>    |
| Do you hold majority shares of organizations located outside of the Member State (incl. EEA/EFTA countries)? | <i>Y/N</i>           |
| If yes, please specify   | <i>Short text</i>    |

|   |     |
|---|-----|
| Does your organization comply to the requirements described in Article 136 of the EU Financial Regulation? <sup>5</sup> (see Annex 3) | Y/N |
| Please review and accept the Confidentiality agreement  | Y/N |
|   |     |

### Representative / Contact Person

|   |                 |
|---|-----------------|
| Name  | Short text      |
| Position  | Short text      |
| Gender  | Multiple choice |
| Email   | Email address   |
| Phone number (personal)   | Phone nr        |
| Please specify the contact person's expertise in the field of cybersecurity | Long text       |

### Fields of Activity / Expertise

|   |                          |
|---|--------------------------|
| Your organizations expertise in the field of cybersecurity (according to Article 8 (3)) | Multiple choice          |
| Expertise - detail description  | Long text                |
| Expertise according to the Cybersecurity Taxonomy                                       | Matrix / multiple choice |
| What do you seek to achieve by joining the  | Long text                |

<sup>5</sup> European Commission, Directorate-General for Budget, Financial regulation applicable to the general budget of the Union : July 2018, Publications Office, 2019, <https://data.europa.eu/doi/10.2761/816722>

|   |                  |
|---|------------------|
| community?  |                  |
| How and in which goals and tasks of community can you contribute? | <i>Long text</i> |

The NCC will process personal data in accordance with the Regulation (EU) 2016/679 and the ECCC will process personal data in accordance with the Regulation (EU) 2018/1725. The legal basis for the processing operation is Article 7 and Article 8 of Regulation (EU) 2021/887.

\*\*\*Additional information on the personal data processed, possible processors and retention periods should be specified by every NCC.

The entity hereby confirms that all information provided in the registration form is truthful and accurate

The entity acknowledges and hereby agrees that the information provided in the registration process will be shared with the ECCC and other NCCs established by each Member State in line with the Regulation

The entity acknowledges and hereby agrees that the following information will be publicly available on the websites of the ECCC and NCCs established by each Member State in line with the Regulation:

- 1) name
- 2) country of establishment
- 3) website
- 4) type of organisation as foreseen in art. 8 para 3 of the Regulation
- 5) fields of activity

#### Disclaimer

|                                |            |
|--------------------------------|------------|
| Article 9 – Tasks of community | <i>Y/N</i> |
| GDPR Conformity                | <i>Y/N</i> |



## **10.2. ANNEX 2 The template to inform about the positive assessment**

Name of the NCC

ECCC

The NCC [NAME] informs the ECCC that the application of [XXXX] was assessed positively according to the Article 8.4 of the Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (Official Journal of the EU 8.06.2021 L 202)

The ECCC is therefore requested to register the [applicant XXX].

A copy of this information will be sent to the applicant XXX.

## **10.3. ANNEX 2 – The Flow chart of the registration process**



#### 10.4. ANNEX 3 – Article 136 of the EU Financial Regulation

Art 136 of the Financial Regulation foresees the following exclusion situations:

(a), the person or entity 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 Union or national law;

(b), it has been established by a final judgment or a final administrative decision that the person or entity 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 judgment or a final administrative decision that the person or entity is guilty of grave professional misconduct by having violated applicable laws or regulations or ethical standards of the profession to which the person or entity belongs, or by having engaged in any wrongful conduct which has an impact on its professional credibility 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 eligibility or selection criteria or in the implementation of the legal commitment;

(ii), entering into agreement with other persons or entities with the aim of distorting competition;

(iii), violating intellectual property rights;

(iv), attempting to influence the decision-making of the authorising officer responsible during the award procedure;

(v), attempting to obtain confidential information that may confer upon it undue advantages in the award procedure;

(d), it has been established by a final judgment that the person or entity is guilty of any of the following:

(i), fraud, within the meaning of Article 3 of Directive (EU) 2017/1371 of the European Parliament and of the Council (44) 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 (45);

(ii), corruption, as defined in Article 4(2) of Directive (EU) 2017/1371 or active corruption within the meaning of 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 (46), or conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA (47), or corruption as defined in other applicable laws;

(iii), conduct related to a criminal organisation as referred to in Article 2 of Council Framework Decision 2008/841/JHA (48);

(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 (49);

(v), terrorist offences or offences linked to terrorist activities, as defined in Articles 1 and 3 of Council Framework Decision 2002/475/JHA (50), 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 (51);

(e), the person or entity has shown significant deficiencies in complying with main obligations in the implementation of a legal commitment financed by the budget which has:

(i), led to the early termination of a legal commitment;

(ii), led to the application of liquidated damages or other contractual penalties; or

(iii), been discovered by an authorising officer, OLAF or the Court of Auditors following checks, audits or investigations;

(f), it has been established by a final judgment or final administrative decision that the person or entity has committed an irregularity within the meaning of Article 1(2) of Council Regulation (EC, Euratom) No 2988/95 (52);

(g), it has been established by a final judgment or final administrative decision that the person or entity has created an entity in 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), it has been established by a final judgment or final administrative decision that an entity has been created with the intent referred to in point (g).