CENTRE FOR CYBERSECURITY BELGIUM

NCC-BE
BELGIUM CYBERSECURITY COORDINATION CENTRE

RULES FOR REGISTRATION AND MEMBERSHIP IN THE NCC-BE COMMUNITY

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

.be

TABLE OF CONTENTS

1. Presentation

The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), the Network of National Coordination Centres (the Network) and the Cybersecurity Competence Community (the Community) together form the new strategic framework for cybersecurity capacity building in the European Union, in accordance with Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs) (the 'Regulation').

1.1. The legal basis of the Guidelines

In accordance with Regulation (EU) 2021/887, the Centre for Cyber Security Belgium has been entrusted with the role of the Cybersecurity Coordination Centre for Belgium ('NCC-BE').
In accordance with decision no. GB/2022/7 of the Management Board of the European Centre for Industrial, Technological and Research Competence in Cybersecurity on the guidelines for membership and registration in the Community and, the current criteria have been created to guide the application and registration process for the Belgian Cybersecurity Community.
The guidelines are established in accordance with section 13.3.i of the Regulations.

1.2. The description of the ECCC

The ECCC is the Union body with legal personality established in 2021 by the above-mentioned Regulation. The ECCC has a dual role: they take on tasks in the field of cybersecurity industry, technology and research, as defined in the Regulation, and manage cybersecurity-related funding under several programmes, in particular Horizon Europe and the Digital Europe Programme. The ECCC is the EU's main instrument to attract investment in cybersecurity research, technology and industrial development and to implement projects and initiatives in collaboration 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 field of cybersecurity by maintaining and developing the EU's research, educational, social, technological and industrial capabilities, as well as the necessary capacities to strengthen trust and security, including data confidentiality, integrity and accessibility, in the Digital Single Market;
2) support the EU's technological capabilities, skills and competences with regard to the resilience and reliability of network and information systems infrastructure, including critical infrastructure and hardware and software commonly used in the EU;
3) increase the global competitiveness of the EU cybersecurity industry and ensure a high level of cybersecurity.

The overall objective of the ECCC is to promote research, innovation and deployment in the field of cybersecurity in order to fulfil its mission. The specific objectives are to:
(1) strengthen cybersecurity capacity, capacities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society, as appropriate;
(2) promote cybersecurity resilience, the adoption of cybersecurity best practices, the principle of security by design and the certification of the security of digital products and services, in a way that complements the efforts of other public entities;
3) contribute to a strong European cybersecurity ecosystem, which brings together all relevant stakeholders.

1.3. The role and tasks of the European Community

The Community contributes to the mission of the ECCC and the Network, by improving, sharing and disseminating cybersecurity expertise across the EU.
The regulation provides that there is only one community in the EU, in which entities from the 27 member states can become members. Nevertheless, it is clear that there is a need for cooperation at a national level as well. The NCCs play a role as guardians of the Community, initially through the application of the evaluation procedure, and then by actively organising and supporting the cooperation of the national members of the Community.
Community **members** have the following tasks:

1) support the ECCC in the fulfilment of their mission and objectives and, to this end, work closely with the ECCC and the National Coordination Centres;
2) where appropriate, participate in formal or informal activities and working groups referred to in point (n) of Article 13(3) in order to carry out specific activities provided for in the annual work programme; and
3) where appropriate, support the ECCC and the national coordination centres in the promotion of specific projects.

The European Community, in particular through the Strategic Advisory Group, shall provide strategic advice to the Executive Director and the Management Board on the agenda, the annual work programme and the multiannual work programme, in accordance with the rules of procedure of the Management Board.
The Community brings together stakeholders who are able to contribute to the mission and who have cybersecurity expertise in the technological, industrial, academic and research fields.
The National Community is composed of:

1) industry, including SMEs;
2) academic and research organizations;
3) other relevant civil society associations;
4) European standardisation organisations;
(5) public entities and other entities dealing with operational and technical cybersecurity issues;
(6) where applicable, stakeholders in sectors that are interested in cybersecurity and face cybersecurity challenges.

The European Community involves:

1) National coordination centres;

2) where applicable, the European Digital Innovation Hubs;

(3) Union institutions, bodies, offices and agencies with relevant expertise, such as ENISA.

2. Membership Criteria

2.1. Formal criteria

2.1.1. The type of entities

Only entities established in the Member States[1] can be members of the European Cybersecurity Competence Community, by contacting the relevant national coordination centre, which translates at Belgian level that only entities legally established under Belgian law are eligible to apply for the Belgian Cybersecurity Competence Community.

Different forms of legal organisation are possible, provided that they comply with Belgian law at the place where the application is submitted.

Establishment implies the actual and effective exercise of the activity through stable arrangements. The legal form of such arrangements, whether they are a branch or a subsidiary with legal personality, is not decisive in that regard[2].

Natural persons acting as ad hoc experts can contribute their expertise when needed and therefore participate in specific activities but cannot be registered as members of the community.

All types of legal entities can be members of the Belgian 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 that are not established in Belgium cannot apply to be part of the Belgian Community.

2.1.2. Cybersecurity expertise

Community members have cybersecurity expertise in at least one of the following areas:

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

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

In order to demonstrate its expertise in cybersecurity, the applicant entity must indicate the type of field in which it is active, accompanied by a description supporting the concrete activities it has carried out.

---

[1] The EEA EFTA States (Iceland, Liechtenstein and Norway) are considered to be Member States when the formal requirements laid down in Council Regulation (EC) No 2894/94 concerning detailed rules for the application of the Agreement on the European Economic Area are fulfilled

[2] C-131/12 Google Spain and Mario Costeja Gonzalez 13 May 2014, C-230/14 Weltimmo 1 October 2014

2.1.3. Assessment on security grounds

Article 8.4 of the Regulation specifies that the assessment shall also take into account any relevant national assessment on security grounds made by the national competent authorities. These registrations are not limited in time but may be revoked at any time by the Competence Centre if the NCC-BE considers that the entity concerned no longer meets the criteria for membership for justified security reasons. In the event of revocation of membership of the Community on security grounds, the decision to revoke shall be proportionate and reasoned.
The purpose of the Community is to be "as open and inclusive as possible, as closed as necessary." The security reasons are therefore a limitation/restriction of access to the Community and, therefore, implementation can be done in specific and well-defined situations and must be clearly stated. This limitation or restriction is assessed by the NCC on a case-by-case basis.
The regulation refers to the national assessment on security grounds, so it is up to the NCC-BE, which receives the request, to identify all relevant factors and apply them to the requesting entity's request. This will be done individually, taking into account the circumstances of the specific case.
The decision to give a negative opinion/rejection on security grounds is a sovereign decision of the NCC-BE. Nevertheless, in order to ensure the harmonisation of the implementation of this provision and to avoid forum shopping, the NCCs should cooperate closely and exchange information. The scope of the information to be shared must be defined by the NCC that received the request. However, when the application receives a negative assessment, this information must be shared without delay within the Network and ECCC.

For security reasons, applications may be rejected or revoked for already registered members of the Community.

2.1.4. Assessment on the basis of the exclusion criteria on the basis of Article 138 of the EU Financial Regulation[3]

The Regulation provides 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 national coordination centre concerned considers that the entity concerned no longer fulfils the criteria set out in paragraph 3 (accession criteria) of this Article or that it falls under Article 138 of the EU Financial Regulation, or for justified security reasons.
Article 138 of the EU Financial Regulation and equivalent national law apply to entities applying to become members of the Community. The entity must not be in a situation of exclusion such as those referred to in Article 138 of the Financial Regulation.
If the entity fulfils one of the conditions listed in Article 138 of the EU Financial Regulation (see Annex 3), its membership may be rejected or revoked immediately, without further assessment. Rejection takes place as a result of the application process to become a member of the community.
The revocation is provided for entities already registered as members of the Community.
The entity should declare, when applying for inclusion as a member of the Community, that

[3] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R1046&qid=1535046024012

none of the exclusion conditions described in Article 138 of the EU Financial Regulation apply to it.
The NCC-BE should in principle be based on the statement provided by the entity. Further analysis is recommended if the NCC-BE suspects the reliability of the statement.
The applicant or member of the Belgian Community shall immediately inform the NCC-BE in writing whether any of the exclusion conditions provided for in Article 138 of the EU Financial Regulation apply.
It should also be required in the application process and furthermore, that only the representative designated by the legal entity under national law (commonly referred to as LEAR) be allowed to sign such a declaration. LEAR also submits to the NCC-BE, every two years, a declaration that none of the conditions listed in Article 138 of the EU Financial Regulation apply.

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

The Regulation provides that the Community must:
• Benefit from the experience and broad representation of relevant stakeholders in the Cybersecurity PPP, ECSO, lessons learned from four pilot projects and the EU FOSSA (Free and Open-Source Software Audits) pilot project.
• Seek exchange with the international community of developments in cybersecurity, including products and processes, standards and technical standards;
• Contribute to the advancement and dissemination of the latest cybersecurity products, services, and processes
• adapt quickly and continuously to new developments in the context of the changing nature of cyber threats and cybersecurity,
• Contribute to the activities of the Competence Centre, the multi-annual work programme and the annual work programme, including through the Strategic Advisory Group.
• The Community should also benefit from the community-building activities of the Competence Centre and the Network
• publicise the fact that their respective activities are carried out within the framework of this Regulation
• ensure that the public and all interested parties receive appropriate, objective, reliable and easily accessible information in a timely manner, in particular with regard to the results of its work. It also makes public the declarations of interests made in accordance with conflicts of interest.
In a broad sense, the Community must contribute to and align itself with the mission of the ECCC and the NCC-BE; Therefore, the applicant entity must describe, at the time of the application for membership, how it will concretely support ECCC and NCC-BE in the achievement of their mission and objectives.
In order to accept or decline an application for membership, the NCC-BE will conduct an assessment of the entity's contribution to the missions of ECCC and NCC to determine whether it is sufficient to pass the assessment.

2.3. Representatives of the entity

The Regulation specifies (Article 8.8) that an entity registered as a member of the Belgian

Community must appoint its representatives in order to ensure an effective dialogue. These representatives have expertise in the field of cyber security research, technology or industry.
In order to streamline the registration process, the entity is advised to appoint the representative already in the online registration form provided by NCC-BE. An entity may appoint one or more representatives, but it must indicate which representative is the primary person representing it. An entity must inform the ECCC and the NCC-BE if the representatives have changed, providing the necessary information for the registration of new representatives.

3. The application process

To apply for membership of the Community, applicants must complete the registration form made available entirely online by the NCC-BE. The form is a common reference point used by all NCCs.

The data provided by the accepted/registered entities will be uploaded to the EU Atlas database, provided by the European Commission.

The application must include information about the entity that allows for an assessment of whether it meets the membership requirements set out in the regulations. In order to simplify the application, during the application process, the entity must identify the representative(s) in the application.

The application will be evaluated by the NCC-BE and other relevant national bodies, and a response will be provided to the applicant.

If necessary, ECCC or the NCC may request additional information or clarification of the request from the entity.

The NCC-BE can involve well-placed actors within the national ecosystem to assist in the evaluation process.

3.1. Evaluation of applications for membership of the Community

In accordance with Article 7.1. (l) of the Regulation, the NCC-BE's mission is to evaluate applications from entities established in Belgium with a view to becoming part of the National Community. Therefore, an entity cannot be registered by the ECCC as a member of the European Cybersecurity Competence Community without a prior assessment by the NCC-BE.

3.1.1. Application Attribution

Applications for membership of the Belgian Community can only be processed by the NCC-BE.

3.1.2. Ensuring balanced representation

NCC-BE will reach out to national stakeholders, through various means, with a particular focus on SMEs, and will actively provide information on the National Community and on the possibility and procedure of joining it.

3.2 Evaluation Schedule

The Regulations do not impose any time limit for either registration or evaluation. Therefore, these administrative processes could take as long as necessary depending on the steps required and the resources available within ECCC/NCC-BE in this area.

The registration process will be open permanently to potential members who can start the process by submitting requests, with the exception of maintenance intervals or technical issues encountered by the registration platform.

3.3. Evaluation results and next steps

Given that the Regulations provide that ECCC will only register entities that have been assessed by a CSC, no further assessment or restriction by ECCC is anticipated. The positive outcome of the NCC's assessment is binding on ECCC, therefore, ECCC cannot refuse to register an entity whose application has been positively assessed by an NCC. The outcome of the NCC's assessment, including any requests for corrections, may be as follows:

3.3.1. Acceptance – positive evaluation

In this case, the NCC-BE shall, without delay, send the registration form together with the information indicating that the result of the assessment has been positive to the ECCC with an application for registration of the entity in the European Cybersecurity Competence Community.

The NCC-BE is not obliged to provide the ECCC with additional reasoning on the reasons for the positive assessment. It should be enough to send the information that the evaluation is positive.

The NCC-BE informs the applicant entity individually (by e-mail or other digital channel) of the successful outcome of the evaluation and submission of the application to the ECCC.

Once the entity has received a positive assessment by the NCC and the information related to the positive assessment with the application has been sent to ECCC, the next step is the official registration issued by ECCC.

Once the registration has been made, the ECCC must inform the entity individually (by email or other digital channel) and all CCNs through a digital platform.

The ECCC should provide a digital register of the members of the European Community. The registry should be public and available on ECCC's website as well as on the NCC websites. The register should be a quick and user-friendly tool for finding entities, in particular by type of entity and country of establishment.

The information provided by an entity in the application, which is necessary for the registration process, will be shared with ECCC. Information provided by an entity during the registration process may be shared with other NCCs.

3.3.2. Rejection – negative assessment

If the conditions described above are not met, the NCC may give a negative assessment. Before issuing a negative assessment, the NCC-BE should endeavour to clarify any errors of interpretation or missing documents with the entity applying for membership in the community.

The result of a negative assessment must be duly justified by the NCC-BE, describing the reasons for the rejection. However, where the negative assessment is carried out on the basis of security grounds, the NCC-BE may decide not to disclose all the circumstances justifying the decision.

Rejected applicants must be given the opportunity to resubmit a new application for membership at any time whenever desired, once their rejection conditions have changed and no earlier than 3 months after a negative assessment.

3.4 Appeal procedure

If an entity has been denied access to the Belgian community, it can choose to appeal the decision. The appeal procedure consists of the following steps:

1) Notification of rejection: The entity receives a formal notification of its rejection, setting out the reasons for the decision, from the NCC-BE. In the notification of rejection, the NCC-BE may request clarification or additional data from the applicant.

2) Request for Appeal: The entity has the opportunity to formally request and submit an appeal of the decision. This formal request must be made in writing and submitted to the NCC-BE within a maximum of 15 calendar days from receipt of the NCC-BE's decision.

3) Forming an Appeal Committee: The public institution that manages the community will establish an appeal committee made up of impartial people who were not involved in the initial decision-making process. This committee could include representatives of, but not limited to, the NCC-BE, members of the Belgian Community, the Belgian Strategic Advisory Group, the Belgian Strategic Council, national security institutions and other experts relevant to the matter.

4) Presentation of the appeal: The rejected entity will present in its written appeal the outline of its case, within the above time frame, including, but not limited to: addressing the reasons for the rejection, providing additional information or evidence, and arguing why the decision should be reconsidered. The appeal must provide the clarifications or data requested by the NCC-BE in the notification of rejection.

5) Review Process: Upon receipt of the formal appeal, the Appeal Panel will undertake a thorough review process, ensuring that it conducts due diligence and considers all relevant factors. The Committee undertakes to complete this assessment within a time frame that allows for a thorough examination of the appeal, including the collection and evaluation of relevant information, consultation with the parties concerned and deliberation to reach a reasoned decision. The committee is committed to upholding the principles of fairness, transparency and procedural integrity throughout this process.

   The Appeals Committee will review the entity's appeal, as well as any relevant documents or evidence provided. They may also request additional information or clarification from both the applicant, the NCC-BE or other relevant bodies supporting the rejection decision.

6) Decision: After careful consideration, the Appeal Committee should render a decision on the entity's appeal. This decision must be communicated in writing to the entity and must be accompanied by clear reasons. The decision of the Appeal Board shall be considered final.

7) Following a negative assessment, the NCC-BE will notify ECCC and the Network of the name of the rejected entity.

This decision may be challenged by an application for annulment before the Council of State within sixty days of its notification. The application must be addressed to the Registry of the Council of State, Rue de la Science 33, 1040 Brussels, either by registered post or via the electronic procedure (see the 'e-Procedure' section of the Council of State's website for further details). If sent by post, the original application must be accompanied by three certified copies, plus one copy for each opposing party.

4. Registration of entities by the ECCC in the European Community

4.1. Registration procedure by the ECCC

The ECCC shall, at their request, register entities as members of the Community after receiving an assessment carried out by the national coordination centre of the Member State in which those entities are established to confirm that they meet the criteria set out in Article 8.3 of the Regulation.

Once the assessment is completed, ECCC is informed of the outcome. The ECCC will acknowledge receipt of the results of the assessment and register all entities that have passed the Belgian assessment process as members of the National Community and then register them as members of the European Community on the ECCC website.

Once the registration has been made, the ECCC must inform the entity individually (by email or other digital channel) and all CCNs through a digital platform.

The list of members of the European Community should be updated regularly.

4.2. The duration of membership of the European Community

Entity records are not time-bound. However, ECCC may revoke membership at any time and provide a relevant written rationale for the decision to the member (see section 5.1 below).

5. Management of accession to the European Community

5.1. Revocation of registration

Entity records are not time-bound. However, the ECCC may revoke membership at any time and provide a relevant written justification for the decision to the member.

If the conditions of membership in the European Community cease to apply in accordance with the conditions of membership set out above, membership is revoked by the CCCB.

The entity should be informed by the ECCC of the initiation of the procedure and given the opportunity to present its position.

Prior to the decision to revoke European membership by the ECCC, an assessment should be carried out by the NCC that provided the assessment at the time of registration. If an entity's place of establishment has changed, the relevant NCC for the assessment must be the place of establishment (see conditions detailed above).

5.2. Withdrawal of membership from members

Any entity wishing to withdraw from the National and/or European Community must formally communicate its intention to the NCC-BE, which will send the withdrawal letter to the ECCC.

5.3. Changes to registration data

The entity must inform the NCC of any changes to the data submitted in the registration form. In particular, changes of representatives, exclusion conditions, contribution to the mission and legal establishment.

Changes to the information provided in the registration form must be submitted to the NCC-BE by the entity using the registration form template. In this case, with the exception of the name, the entity should only fill in the fields on the form where the changes took place.

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

6. Coordination and cooperation between the NCCs

The NCCs serve as contact points at national level for the Community to help the ECCC fulfil its mission and objectives.

Given that potential members of the Community may operate and provide services throughout the Union, be established in several Member States or be linked to other potential members of the Community in other Member States (including in the form of subsidiaries or partner companies), the NCCs should coordinate and cooperate through the network in order to find a mutually aligned way of building the Community.

There may 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 to the NCC of another Member State, notwithstanding the requirements relating to establishment. This would run counter to the first assessment and the rejection decision and could undermine confidence in the Community as a whole.

In the case of an entity or subsidiaries of a group of companies operating simultaneously in several Member States, the respective CCNs must engage in a close dialogue with each other in order to ensure a consistent assessment procedure, recognising that there may be circumstances where subsidiaries located in different Member States may make different contributions to the mission and have different types of cybersecurity expertise.

The NCCs will share information on pending applications as well as rejected applications as soon as possible.

APPENDIX 1 – Registration Form (available to members of the NCC-BE Community Registration Platform)[4]

Your organization

Please note that fields marked with * are mandatory

Name in the national language *	*Short text*
Name in English *	*Short text*
Entity/Department (if applicable)	*Short text*
Address *	*Short text*
Company / organization registration number	*Alphanumeric*
Is this your organization's main seat / headquarter?	*Y/N*
If not, please provide the name and address of the main seat / headquarter *(*) Mandatory if above is N*	*Short text*
Website *	*URL*
Phone number	*Phone nr.*
Email *	*Email address*
Organization type * *(single choice)*	• product supplier/service provider (industry) • academic and research organisation • civil society organisation/business association • European standardisation organisation • public entity/administration/state service • stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges

[4] In accordance with DECISION No GB/2025/5 of the Governing Board of the European Centre for Industrial, Technological and Research Competence in Cybersecurity on the amendment of Annex 1 to DECISION No GB/2022/7.

Does your organization have subsidiaries in other EU Member States (including EEA/EFTA countries)	*Y/N*
If yes, please specify *(*) mandatory if above is Y*	*Short text*
Do you hold majority shares of organizations located outside of the Member State (incl. EEA/EFTA countries)?	*Y/N*
If yes, please specify *(*) mandatory if above is Yes*	*Short text*
Does your organization comply to the requirements described in Article 138 of the EU Financial Regulation?[5] (see Annex 3) *[2]	*Y/N*
Please review and accept the Confidentiality and Data Protection Notes included below. *	*Y/N*

Representative / Contact Person

Name *	*Short text*
Surname *	*Short text*
Position	*Short text*
Email *	*Email address*
Phone number (direct)	*Phone nr*

Fields of Activity / Expertise

Your organization's expertise in the field of cybersecurity (according to Article 8 (3) * (multiple choice)	*(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*
Expertise - detail description *	*Long text*
Expertise according to the Cybersecurity Taxonomy	*Matrix / multiple choice*
What do you seek to achieve by joining the community?	*Long text*
How and in which goals and tasks of community can you contribute?	*Long text*

Please note that when filling in the form, the address fields need to comply with the following requirements:

- Country: use only the country of your NCC as provided in the predefined list.
- Street address: only street name and house number. Please do not add zip code, info about buildings, floor etc.
- Do not insert additional commas, symbols or other words
- Ensure the information provided is correct and written correctly.
- City: add only the name of the city. Please do not repeat the country, nor add zip code
- Do not invert city and street, repeat street or city twice.

The NCC-BE will process the personal data in accordance with Regulation (EU) 2016/679 (GDPR) and the ECCC will process the personal data in accordance with Regulation (EU) 2018/1725 (EUDPR). The legal basis for the processing operation is Article 6(1)(e) of the GDPR and Article 5(1)(a) of the GDPR on the basis of Articles 7 and 8 of Regulation (EU) 2021/887.
More information on the privacy policy can be found on the website of the Centre for Cyber Security Belgium, the parent organisation of the NCC-BE.

The entity applying for registration with the NCC-BE community hereby confirms that all information provided in the registration form is true and accurate.
The entity hereby 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 accordance with the Regulation and will not be shared further.
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 provided for in Article 8 paragraph 2 of the Regulation
5) Areas of activity.

APPENDIX 2 The Positive Assessment Information Model

From: NCC-BE

To: ECCC

The NCC - BE informs the ECCC that the application for [XXXX] has been positively assessed in accordance with Article 8.4 of 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 [applicant XXX].

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

ANNEX 3 – Article 138 of the EU Financial Regulation[5]

The article 138 of the Financial Regulation stipulates 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) unduly influencing or attempting to unduly influence the decision-making process to obtain Union funds by taking advantage, through misrepresentation, of a conflict of interests involving any financial actors or other persons referred to in Article 61(1);

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

[5] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) - https://eur-lex.europa.eu/eli/reg/2024/2509/oj/eng

(vi) incitement to discrimination, hatred or violence against a group of persons or a member of a group or similar activities that are contrary to the values on which the Union is founded enshrined in Article 2 TEU, where such misconduct has an impact on the person or entity's integrity which negatively affects or concretely risks affecting the performance of the legal commitment;

(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 (49) 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 (50);

(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 (51), or conduct referred to in Article 2(1) of Council Framework Decision 2003/568/JHA (52), 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 (53);

(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 (54);

(v) terrorist offences or offences related to terrorist activities, as defined in Articles 3 to 12 of Directive (EU) 2017/541 of the European Parliament and of the Council (55), or inciting, aiding, abetting or attempting to commit such offences, as referred to in Article 14 of that Directive;

(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 (56);

(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, the Court of Auditors, or the EPPO 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 (57);

(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, including those related to working rights, employment and labour conditions, 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);

(i) the entity or person has intentionally and without proper justification resisted an investigation, check or audit carried out by an authorising officer or its representative or auditor, OLAF, the EPPO, or the Court of Auditors. It shall be considered that the person or entity resists an investigation, check or audit when it carries out actions with the goal or effect of preventing, hindering or delaying the conduct of any of the activities needed to perform the investigation, check or audit. Such actions shall include, in particular, refusing to grant the necessary access to its premises or any other areas used for business purposes, concealing or refusing to disclose information or providing false information.