CENTRE FOR CYBERSECURITY BELGIUM

NCC-BE
BELGIUM CYBERSECURITY COORDINATION CENTRE

RÈGLES D'INSCRIPTION ET D'ADHÉSION À LA COMMUNAUTÉ NCC-BE

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 DES MATIÈRES

1. Présentation

Le centre européen de compétences industrielles, technologiques et de recherche (CETC) en cybersécurité, le réseau de centres nationaux de coordination (le réseau) et la communauté de compétences en cybersécurité (la communauté) forment ensemble le nouveau cadre stratégique pour le renforcement des capacités en matière de cybersécurité dans l'Union européenne, conformément au règlement (UE) 2021/887 établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité (CETC) et le Réseau des centres nationaux de coordination (CCN) (ci-après le « règlement »).

1.1. La base juridique des lignes directrices

Conformément au règlement (UE) 2021/887, le Centre pour la cybersécurité Belgique s'est vu confier le rôle de Centre de coordination de la cybersécurité pour la Belgique (NCC-BE).
Conformément à la décision n°. GB/2022/7 du Conseil d'administration du Centre européen de compétences industrielles, technologiques et de recherche en cybersécurité sur les lignes directrices pour l'adhésion et l'enregistrement dans la Communauté et les critères actuels ont été créés pour guider le processus de candidature et d'inscription à la Communauté belge de cybersécurité.
Les lignes directrices sont établies conformément à l'article 13.3.i du Règlement.

1.2. La description des CETC

Les CETC sont l'organe de l'Union doté de la personnalité juridique créé en 2021 par le règlement susmentionné. Les CETC ont un double rôle : ils assument des tâches dans le domaine de l'industrie, de la technologie et de la recherche en matière de cybersécurité, tels que définis dans le règlement, et gèrent les financements liés à la cybersécurité dans le cadre de plusieurs programmes, en particulier Horizon Europe et le programme pour une Europe numérique. Les CETC sont le principal instrument de l'UE pour attirer des investissements dans la recherche, la technologie et le développement industriel en matière de cybersécurité et pour mettre en œuvre des projets et des initiatives en collaboration avec le réseau.
La mission des CETC et du réseau est d'aider l'UE à :

1) renforcer son leadership et son autonomie stratégique dans le domaine de la cybersécurité en maintenant et en développant les capacités de l'UE en matière de recherche, d'éducation, sociales, technologiques et industrielles, ainsi que les capacités nécessaires pour renforcer la confiance et la sécurité, y compris la confidentialité, l'intégrité et l'accessibilité des données, dans le marché unique numérique ;
2) soutenir les capacités, les aptitudes et les compétences technologiques de l'UE en ce qui concerne la résilience et la fiabilité des infrastructures de réseau et des systèmes d'information, y compris les infrastructures critiques et le matériel et les logiciels couramment utilisés dans l'UE ;

3) accroître la compétitivité mondiale de l'industrie de la cybersécurité de l'UE et garantir un niveau élevé de cybersécurité.

L'objectif général des CETC est de promouvoir la recherche, l'innovation et le déploiement dans le domaine de la cybersécurité afin de remplir sa mission. Les objectifs spécifiques sont les suivants :
(1) renforcer les capacités, les capacités, les connaissances et les infrastructures en matière de cybersécurité dans l'intérêt de l'industrie, en particulier des PME, des communautés de recherche, du secteur public et de la société civile, le cas échéant ;
(2) promouvoir la résilience en matière de cybersécurité, l'adoption de bonnes pratiques en matière de cybersécurité, le principe de la sécurité dès la conception et la certification de la sécurité des produits et services numériques, d'une manière qui complète les efforts d'autres entités publiques ;
3) contribuer à un écosystème européen de cybersécurité solide, qui rassemble toutes les parties prenantes concernées.

1.3. Le rôle et les tâches de la Communauté européenne

La Communauté contribue à la mission des CETC et du réseau en améliorant, en partageant et en diffusant l'expertise en matière de cybersécurité dans l'ensemble de l'UE.
Le règlement prévoit qu'il n'y a qu'une seule communauté dans l'UE, à laquelle les entités des 27 États membres peuvent devenir membres. Néanmoins, il est clair qu'il est également nécessaire d'instaurer une coopération au niveau national. Les CCN jouent un rôle de gardiens de la Communauté, d'abord par l'application de la procédure d'évaluation, puis en organisant et en soutenant activement la coopération des membres nationaux de la Communauté.
Les membres de **la communauté** ont les tâches suivantes :

1) soutenir les CETC dans la réalisation de leur mission et de leurs objectifs et, à cette fin, travailler en étroite collaboration avec les CETC et les centres nationaux de coordination ;
2) le cas échéant, participer aux activités formelles ou informelles et aux groupes de travail visés à l'article 13, paragraphe 3, point n), afin de mener à bien des activités spécifiques prévues dans le programme de travail annuel ; et
3) le cas échéant, soutenir les CETC et les centres nationaux de coordination dans la promotion de projets spécifiques.

La Communauté européenne, notamment par l'intermédiaire du groupe consultatif stratégique, fournit des conseils stratégiques au directeur exécutif et au conseil d'administration sur l'ordre du jour, le programme de travail annuel et le programme de travail pluriannuel, conformément au règlement intérieur du conseil d'administration.
La Communauté rassemble des parties prenantes qui sont en mesure de contribuer à la mission et qui ont une expertise en cybersécurité dans les domaines technologiques, industriels, académiques et de la recherche.
La Communauté Nationale est composée de :

1) l'industrie, y compris les PME ;

2) les organisations universitaires et de recherche ;
3) d'autres associations de la société civile concernées ;
4) les organisations européennes de normalisation ;
(5) les entités publiques et autres entités traitant de questions opérationnelles et techniques de cybersécurité ;
(6) le cas échéant, les parties prenantes des secteurs qui s'intéressent à la cybersécurité et qui sont confrontés à des défis en matière de cybersécurité.

La Communauté européenne implique :

1) Centres nationaux de coordination ;
2) le cas échéant, les pôles européens d'innovation numérique ;
(3) Les institutions, organes et organismes de l'Union disposant d'une expertise pertinente, tels que l'ENISA.

2. Critères d'adhésion

2.1. Critères formels

2.1.1. Le type d'entités

Seules les entités établies dans les États membres[1] peuvent être membres de la Communauté européenne de compétences en cybersécurité, en contactant le centre de coordination national compétent, ce qui traduit au niveau belge que seules les entités légalement établies en vertu du droit belge sont éligibles pour postuler à la Communauté belge de compétences en cybersécurité.

Différentes formes d'organisation juridique sont possibles, à condition qu'elles soient conformes au droit belge du lieu d'introduction de la demande.

L'établissement implique l'exercice effectif et effectif de l'activité par le biais d'arrangements stables. La forme juridique d'un tel montage, qu'il s'agisse d'une succursale ou d'une filiale dotée de la personnalité juridique, n'est pas déterminante à cet égard[2].

Les personnes physiques agissant en tant qu'experts ad hoc peuvent apporter leur expertise en cas de besoin et donc participer à des activités spécifiques, mais ne peuvent pas être enregistrées en tant que membres de la communauté.

Tous les types de personnes morales peuvent être membres de la communauté belge, y compris, mais sans s'y limiter :

1) les entités du secteur public ;
2) les entités du secteur privé ;
3) les associations, organisations et organismes collectifs ;
4) les organisations à but non lucratif.

Les entités qui ne sont pas établies en Belgique ne peuvent pas demander à faire partie de la Communauté belge.

2.1.2. Expertise en cybersécurité

Les membres de la communauté possèdent une expertise en cybersécurité dans au moins l'un des domaines suivants :

1) le milieu universitaire, la recherche ou l'innovation ;
2) le développement industriel ou de produits ;
3) la formation et l'éducation ;
4) les opérations de sécurité de l'information ou de réponse aux incidents ;
5) l'éthique ;
6) Normalisation et spécifications formelles et techniques.

La notion d'expertise nécessite un certain niveau de connaissances ou de compétences. Par conséquent, une entité doit être en mesure de démontrer qu'elle a été active dans un ou plusieurs des domaines énumérés ci-dessus.

Afin de démontrer son expertise en matière de cybersécurité, l'entité candidate doit indiquer

[1] Les États de l'AELE de l'EEE (Islande, Liechtenstein et Norvège) sont considérés comme des États membres lorsque les conditions de forme prévues par le règlement (CE) n° 2894/94 du Conseil concernant les modalités d'application de l'accord sur l'Espace économique européen sont remplies

[2] C-131/12 Google Espagne et Mario Costeja Gonzalez 13 mai 2014, C-230/14 Weltimmo 1er octobre 2014

le type de domaine dans lequel elle est active, accompagnée d'une description à l'appui des activités concrètes qu'elle a menées.

2.1.3. Évaluation pour des raisons de sécurité

L'article 8.4 du règlement précise que l'évaluation tient également compte de toute évaluation nationale pertinente pour des raisons de sécurité effectuée par les autorités nationales compétentes. Ces enregistrements ne sont pas limités dans le temps, mais peuvent être révoqués à tout moment par le centre de compétences si le NCC-BE estime que l'entité concernée ne remplit plus les critères d'adhésion pour des raisons de sécurité justifiées. En cas de révocation de l'adhésion à la Communauté pour des raisons de sécurité, la décision de révocation est proportionnée et motivée.

Le but de la Communauté est d'être « aussi ouvert et inclusif que possible, aussi fermé que nécessaire ». Les raisons de sécurité sont donc une limitation/restriction de l'accès à la Communauté et, par conséquent, la mise en œuvre peut se faire dans des situations spécifiques et bien définies et doit être clairement énoncée. Cette limitation ou restriction est évaluée par la CCN au cas par cas.

Le règlement fait référence à l'évaluation nationale pour des raisons de sécurité, il appartient donc au NCC-BE, qui reçoit la demande, d'identifier tous les facteurs pertinents et de les appliquer à la demande de l'entité requérante. Cela se fera individuellement, en tenant compte des circonstances du cas d'espèce.

La décision de donner un avis négatif/rejet pour des raisons de sécurité est une décision souveraine du NCC-BE. Néanmoins, afin d'assurer l'harmonisation de la mise en œuvre de cette disposition et d'éviter le forum shopping, les CCN devraient coopérer étroitement et échanger des informations. La portée de l'information à partager doit être définie par la CCN qui a reçu la demande. Toutefois, lorsque la demande reçoit une évaluation négative, cette information doit être partagée sans délai au sein du Réseau et d'ECCC.

Pour des raisons de sécurité, les demandes peuvent être rejetées ou révoquées pour les membres déjà inscrits dans la Communauté.

2.1.4. Évaluation sur la base des critères d'exclusion sur la base de l'article 136 du règlement financier de l'UE[3]

L'article 8.4 du règlement prévoit que les enregistrements ne sont pas limités dans le temps, mais peuvent être révoqués par le centre de compétences à tout moment si le centre national de coordination concerné estime que l'entité concernée ne remplit plus les critères énoncés au paragraphe 3 (critères d'adhésion) du présent article ou qu'elle relève de l'article 136 du règlement financier de l'UE, ou pour des raisons de sécurité justifiées.

L'article 136 du règlement financier de l'UE et le droit national équivalent s'appliquent aux entités qui demandent à devenir membres de la Communauté. L'entité ne doit pas se trouver dans une situation d'exclusion telle que celles visées à l'article 136 du règlement financier.

Si l'entité remplit l'une des conditions énumérées à l'article 136 du règlement financier de l'UE

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

(voir annexe 3), son adhésion peut être rejetée ou révoquée immédiatement, sans autre évaluation. Le rejet a lieu à la suite du processus de demande pour devenir membre de la communauté.
La révocation est prévue pour les entités déjà enregistrées en tant que membres de la Communauté.
L'entité devrait déclarer, lorsqu'elle demande à être membre de la Communauté, qu'aucune des conditions d'exclusion décrites à l'article 136 du règlement financier de l'UE ne s'applique à elle.
Le NCC-BE devrait en principe être basé sur la déclaration fournie par l'entité. Une analyse plus approfondie est recommandée si le NCC-BE soupçonne la fiabilité de l'affirmation.
Le demandeur ou le membre de la Communauté belge informe immédiatement et par écrit le NCC-BE si l'une des conditions d'exclusion prévues à l'article 136 du règlement financier de l'UE s'applique.
Il devrait également être exigé dans le processus de demande et, en outre, que seul le représentant désigné par la personne morale en vertu du droit national (communément appelé LEAR) soit autorisé à signer une telle déclaration. En outre, tous les deux ans, le LEAR soumet au NCC-BE une déclaration selon laquelle aucune des conditions énumérées à l'article 136 du règlement financier de l'UE ne s'applique.

2.2. Contribution à la mission des CETC et du Réseau

Le règlement prévoit que la Communauté doit :
• Bénéficier de l'expérience et d'une large représentation des parties prenantes concernées dans le PPP de cybersécurité, ECSO, des leçons tirées de quatre projets pilotes et du projet pilote FOSSA (Free and Open-Source Software Audits) de l'UE.
• Rechercher l'échange avec la communauté internationale sur les développements en matière de cybersécurité, y compris les produits et processus, les normes et les normes techniques ;
• Contribuer à l'avancement et à la diffusion des derniers produits, services et processus de cybersécurité
• s'adapter rapidement et en permanence aux nouvelles évolutions dans le contexte de la nature changeante des cybermenaces et de la cybersécurité,
• Contribuer aux activités du Centre de compétences, au programme de travail pluriannuel et au programme de travail annuel, notamment par l'intermédiaire du Groupe consultatif stratégique.
• La Communauté devrait également bénéficier des activités de renforcement de la communauté du Centre de compétences et du Réseau.
• faire connaître le fait que leurs activités respectives sont exercées dans le cadre du présent règlement
• veiller à ce que le public et toutes les parties intéressées reçoivent en temps utile des informations appropriées, objectives, fiables et facilement accessibles, en particulier en ce qui concerne les résultats de ses travaux. Il rend également publiques les déclarations d'intérêts faites en matière de conflits d'intérêts.
Au sens large, la Communauté doit contribuer à la mission des CETC et du NCC-BE et s'aligner sur celle-ci. Par conséquent, l'entité candidate doit décrire, au moment de la demande d'adhésion, comment elle soutiendra concrètement ECCC et NCC-BE dans la réalisation de leur

mission et de leurs objectifs.
Afin d'accepter ou de refuser une demande d'adhésion, le NCC-BE procédera à une évaluation de la contribution de l'entité aux missions d'ECCC et de NCC afin de déterminer si elle est suffisante pour réussir l'évaluation.

2.3. Représentants de l'entité

Le Règlement précise (article 8.8) qu'une entité enregistrée en tant que membre de la Communauté belge doit désigner ses représentants afin d'assurer un dialogue effectif. Ces représentants ont une expertise dans le domaine de la recherche, de la technologie ou de l'industrie en cybersécurité.
Afin de simplifier le processus d'enregistrement, il est conseillé à l'entité de désigner le représentant déjà dans le formulaire d'inscription en ligne fourni par NCC-BE. Une entité peut désigner un ou plusieurs représentants, mais elle doit indiquer quel représentant est la personne qui la représente principalement. Une entité doit informer les CETC et le NCC-BE si les représentants ont changé, en fournissant les informations nécessaires à l'enregistrement de nouveaux représentants.

3. Le processus de candidature

Pour demander leur adhésion à la Communauté, les candidats doivent remplir le formulaire d'inscription mis à disposition entièrement en ligne par le NCC-BE. Le formulaire est un point de référence commun utilisé par toutes les CCN.

Les données fournies par les entités acceptées/enregistrées seront téléchargées dans la base de données Atlas de l'UE, fournie par la Commission européenne.

La demande doit comprendre des renseignements sur l'entité qui permettent d'évaluer si elle satisfait aux exigences d'adhésion énoncées dans les règlements. Afin de simplifier la demande, au cours du processus de demande, l'entité doit identifier le ou les représentants dans la demande.

La demande sera évaluée par le NCC-BE et d'autres organismes nationaux compétents, et une réponse sera fournie au demandeur.

Au besoin, ECCC ou la CCN peut demander des renseignements supplémentaires ou des éclaircissements à l'entité.

Le NCC-BE peut impliquer des acteurs bien placés au sein de l'écosystème national pour aider au processus d'évaluation.

3.1. Évaluation des demandes d'adhésion à la Communauté

Conformément à l'article 7.1. (l) du Règlement, la NCC-BE a pour mission d'évaluer les demandes émanant d'entités établies en Belgique en vue de faire partie de la Communauté Nationale. Par conséquent, une entité ne peut pas être enregistrée par les CETC en tant que membre de la communauté européenne de compétences en cybersécurité sans une évaluation préalable par le NCC-BE.

3.1.1. Attribution de l'application

Les demandes d'adhésion à la Communauté belge ne peuvent être traitées que par le NCC-BE.

3.1.2. Assurer une représentation équilibrée

Le NCC-BE s'adressera aux parties prenantes nationales, par divers moyens, en mettant l'accent sur les PME, et fournira activement des informations sur la communauté nationale et sur la possibilité et la procédure d'y adhérer.

3.2 Calendrier de l'évaluation

Le Règlement n'impose aucune limite de temps pour l'inscription ou l'évaluation. Par conséquent, ces processus administratifs pourraient prendre aussi de temps que nécessaire selon les étapes requises et les ressources disponibles au sein d'ECCC/NCC-BE dans ce domaine.

Le processus d'inscription sera ouvert de manière permanente aux membres potentiels qui pourront commencer le processus en soumettant des demandes, à l'exception des intervalles de maintenance ou des problèmes techniques rencontrés par la plateforme d'inscription.

3.3. Résultats de l'évaluation et prochaines étapes

Étant donné que le Règlement prévoit qu'ECCC n'enregistrera que les entités qui ont été évaluées par un SCC, aucune autre évaluation ou restriction de la part d'ECCC n'est prévue. Le résultat positif de l'évaluation de la CCN est contraignant pour ECCC, par conséquent, ECCC ne peut pas refuser d'enregistrer une entité dont la demande a été évaluée positivement par une CCN. Le résultat de l'évaluation de la CCN, y compris toute demande de correction, peut être le suivant :

3.3.1. Acceptation – évaluation positive

Dans ce cas, le NCC-BE envoie sans délai le formulaire d'inscription accompagné des informations indiquant que le résultat de l'évaluation a été positif aux CETC avec une demande d'enregistrement de l'entité dans la communauté européenne de compétences en cybersécurité.

Le NCC-BE n'est pas tenu de fournir aux ECCC un raisonnement supplémentaire sur les raisons de l'évaluation positive. Il devrait suffire d'envoyer l'information que l'évaluation est positive.

Le NCC-BE informe l'entité candidate individuellement (par e-mail ou par un autre canal numérique) de l'issue positive de l'évaluation et de la soumission de la demande aux CETC.

Une fois que l'entité a reçu une évaluation positive de la part de la CCN et que les renseignements relatifs à l'évaluation positive avec la demande ont été envoyés à ECCC, l'étape suivante est l'enregistrement officiel délivré par ECCC.

Une fois l'enregistrement effectué, les CETC doivent informer l'entité individuellement (par courriel ou par un autre canal numérique) et tous les NCF par le biais d'une plateforme numérique.

Les CETC devraient fournir un registre numérique des membres de la Communauté européenne. Le registre devrait être public et disponible sur le site Web d'ECCC ainsi que sur les sites Web de la CCN. Le registre devrait être un outil rapide et convivial permettant de trouver des entités, en particulier par type d'entité et par pays d'établissement.

Les renseignements fournis par une entité dans la demande, qui sont nécessaires au processus d'inscription, seront partagés avec ECCC. Les renseignements fournis par une entité au cours du processus d'inscription peuvent être partagés avec d'autres CCN.

3.3.2. Rejet – évaluation négative

Si les conditions décrites ci-dessus ne sont pas remplies, la CCN peut donner une évaluation négative. Avant d'émettre une évaluation négative, le NCC-BE doit s'efforcer de clarifier toute erreur d'interprétation ou tout document manquant avec l'entité qui demande l'adhésion à la communauté.

Le résultat d'une évaluation négative doit être dûment justifié par le NCC-BE, en décrivant les raisons du rejet. Toutefois, lorsque l'évaluation négative est effectuée sur la base de raisons de sécurité, le NCC-BE peut décider de ne pas divulguer toutes les circonstances justifiant la décision.

Les candidats rejetés doivent avoir la possibilité de soumettre à nouveau une nouvelle demande d'adhésion à tout moment lorsqu'ils le souhaitent, une fois que leurs conditions de rejet ont changé et au plus tôt 3 mois après une évaluation négative.

3.4 Procédure de recours

Si une entité s'est vu refuser l'accès à la communauté belge, elle peut choisir de faire appel de la décision. La procédure de recours comprend les étapes suivantes :

1) Notification de rejet : L'entité reçoit une notification formelle de son rejet, exposant les motifs de la décision, de la part du NCC-BE. Dans la notification de rejet, le NCC-BE peut demander des éclaircissements ou des données supplémentaires au demandeur.

2) Demande d'appel : L'entité a la possibilité de demander officiellement et de soumettre un appel de la décision. Cette demande formelle doit être formulée par écrit et soumise au NCC-BE dans un délai maximum de 15 jours calendaires à compter de la réception de la décision du NCC-BE.

3) Formation d'un comité d'appel : L'établissement public qui gère la communauté mettra sur pied un comité d'appel composé de personnes impartiales qui n'ont pas participé au processus décisionnel initial. Ce comité pourrait comprendre des représentants, mais sans s'y limiter, du NCC-BE, des membres de la Communauté belge, du Groupe consultatif stratégique belge, du Conseil stratégique belge, des institutions nationales de sécurité et d'autres experts pertinents en la matière.

4) Présentation de l'appel : L'entité rejetée présentera dans son appel écrit les grandes lignes de son dossier, dans le délai ci-dessus, y compris, mais sans s'y limiter : aborder les raisons du rejet, fournir des informations ou des preuves supplémentaires, et argumenter pourquoi la décision devrait être réexaminée. Le recours doit fournir les éclaircissements ou les données demandés par le NCC-BE dans la notification de rejet.

5) Processus d'examen : À la réception de l'appel officiel, le comité d'appel entreprendra un processus d'examen approfondi, en s'assurant qu'il fait preuve de diligence raisonnable et tient compte de tous les facteurs pertinents. Le Comité s'engage à mener à bien cette évaluation dans un délai qui permette un examen approfondi du recours, y compris la collecte et l'évaluation des informations pertinentes, la consultation des parties concernées et la délibération en vue de parvenir à une décision motivée. Le comité s'est engagé à respecter les principes d'équité, de transparence et d'intégrité procédurale tout au long de ce processus.
   Le comité d'appel examinera l'appel de l'entité, ainsi que tout document ou preuve pertinent fourni. Ils peuvent également demander des informations supplémentaires ou des éclaircissements à la fois au demandeur, au NCC-BE ou à d'autres organismes compétents soutenant la décision de rejet.

6) Décision : Après un examen attentif, le comité d'appel devrait rendre une décision sur l'appel de l'entité. Cette décision doit être communiquée par écrit à l'entité et doit être accompagnée de motifs clairs. La décision du comité d'appel est considérée comme définitive.

7) À la suite d'une évaluation négative, le NCC-BE informera ECCC et le réseau du nom de l'entité rejetée.

4. Enregistrement des entités par les CETC dans la Communauté européenne

4.1.La procédure d'enregistrement par les CETC

À leur demande, les CETC enregistrent les entités en tant que membres de la Communauté après avoir reçu une évaluation effectuée par le centre national de coordination de l'État membre dans lequel ces entités sont établies pour confirmer qu'elles répondent aux critères énoncés à l'article 8.3 du règlement.

Une fois l'évaluation terminée, ECCC est informé du résultat. Les CETC accuseront réception des résultats de l'évaluation et enregistreront toutes les entités qui ont réussi le processus d'évaluation belge en tant que membres de la Communauté nationale, puis les enregistreront en tant que membres de la Communauté européenne sur le site web des ECCC.

Une fois l'enregistrement effectué, les CETC doivent informer l'entité individuellement (par courriel ou par un autre canal numérique) et tous les NCF par le biais d'une plateforme numérique.

La liste des membres de la Communauté européenne devrait être mise à jour régulièrement.

4.2. La durée de l'adhésion à la Communauté européenne

Les enregistrements d'entité ne sont pas limités dans le temps. Toutefois, ECCC peut révoquer l'adhésion à tout moment et fournir au membre une justification écrite pertinente de sa décision (voir la section 5.1 ci-dessous).

5. La gestion de l'adhésion à la Communauté européenne

5.1. Révocation de l'inscription

Les enregistrements d'entité ne sont pas limités dans le temps. Toutefois, ECCC peut révoquer l'adhésion à tout moment et fournir au membre une justification écrite pertinente de sa décision.

Si les conditions d'adhésion à la Communauté européenne cessent de s'appliquer conformément aux conditions d'adhésion énoncées ci-dessus, l'adhésion est révoquée par la CECC.

L'entité devrait être informée par les CETC de l'ouverture de la procédure et avoir la possibilité de présenter sa position.

Avant la décision de révoquer l'adhésion européenne par les CECC, une évaluation devrait être effectuée par le CNC qui a fourni l'évaluation au moment de l'enregistrement. Si le lieu d'établissement d'une entité a changé, le NCC pertinent pour l'évaluation doit être le lieu d'établissement (voir les conditions détaillées ci-dessus).

5.2. Retrait de l'adhésion des membres

Toute entité souhaitant se retirer de la Communauté nationale et/ou européenne doit communiquer formellement son intention au NCC-BE, qui enverra la lettre de retrait aux CETC.

5.3. Modifications des données d'inscription

L'entité doit informer la CCN de toute modification des données soumises dans le formulaire d'inscription. Notamment, les changements de représentants, les conditions d'exclusion, la contribution à la mission et l'établissement juridique.

Les modifications apportées aux informations fournies dans le formulaire d'inscription doivent être soumises au NCC-BE par l'entité à l'aide du modèle de formulaire d'enregistrement. Dans ce cas, à l'exception du nom, l'entité ne doit renseigner que les champs du formulaire où les modifications ont eu lieu.

Le NCC-BE évalue les changements et envoie le formulaire à ECCC pour refléter les changements dans le registre.

6. Coordination et coopération entre les CCN

Les CCN servent de points de contact au niveau national pour la Communauté afin d'aider les CETC à remplir leur mission et leurs objectifs.
Étant donné que les membres potentiels de la Communauté peuvent opérer et fournir des services dans l'ensemble de l'Union, être établis dans plusieurs États membres ou être liés à d'autres membres potentiels de la Communauté dans d'autres États membres (y compris sous la forme de filiales ou d'entreprises partenaires), les CCN devraient se coordonner et coopérer par l'intermédiaire du réseau afin de trouver une manière mutuellement alignée de construire la Communauté.
Il peut y avoir des situations où une entité dont la demande d'adhésion est rejetée par le NCC d'un État membre s'efforce de demander son adhésion au NCC d'un autre État membre, nonobstant les exigences relatives à l'établissement. Cela irait à l'encontre de la première évaluation et de la décision de rejet et pourrait saper la confiance dans la Communauté dans son ensemble.
Dans le cas d'une ou de plusieurs filiales d'un groupe de sociétés opérant simultanément dans plusieurs États membres, les CCN respectifs doivent engager un dialogue étroit entre eux afin d'assurer une procédure d'évaluation cohérente, en reconnaissant qu'il peut y avoir des circonstances dans lesquelles des filiales situées dans différents États membres peuvent apporter des contributions différentes à la mission et disposer de différents types d'expertise en matière de cybersécurité.
Les CCN partageront dès que possible de l'information sur les demandes en attente ainsi que sur les demandes rejetées.

ANNEXE 1 – Formulaire d'inscription (disponible pour les membres de la plateforme d'inscription communautaire NCC-BE)[4]

Votre organisation

Veuillez noter que les champs marqués d'un * sont obligatoires

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] Conformément à la décision n° GB/2025/5 du conseil d'administration du Centre européen de compétences industrielles, technologiques et de recherche en cybersécurité relative à la modification de l'annexe 1 de la décision n° 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*

Le NCC-BE traitera les données à caractère personnel conformément au règlement (UE) 2016/679 (RGPD) et les CETC traiteront les données à caractère personnel conformément au règlement (UE) 2018/1725 (EUDPR). La base juridique de l'opération de traitement est l'article 6, paragraphe 1, point e), du RGPD et l'article 5, paragraphe 1, point a), du RGPD sur la base des articles 7 et 8 du règlement (UE) 2021/887.
Vous trouverez de plus amples informations sur la politique de confidentialité sur le site web du Centre pour la cybersécurité Belgique, l'organisation mère du NCC-BE.

L'entité qui demande à s'inscrire auprès de la communauté NCC-BE confirme par la présente que toutes les informations fournies dans le formulaire d'inscription sont véridiques et exactes.
L'entité reconnaît et accepte par la présente que les informations fournies dans le cadre du processus d'enregistrement seront partagées avec les CETC et les autres CCN établis par chaque État membre conformément au Règlement et ne seront pas partagées par la suite.
L'entité reconnaît et accepte par la présente que les informations suivantes seront mises à la disposition du public sur les sites web des CETC et des CCN établis par chaque État membre conformément au règlement :
1) Nom
2) Pays d'établissement
3) Site web
4) Type d'organisation prévu à l'article 8, paragraphe 2, du règlement
5) Domaines d'activité.

ANNEXE 2 Le modèle d'information sur l'évaluation positive

De : NCC-BE

Destinataire : ECCC

Le NCC - BE informe les CETC que la demande de [XXXX] a été évaluée positivement conformément à l'article 8.4 du règlement (UE) 2021/887 du Parlement européen et du Conseil du 20 mai 2021 établissant le Centre européen de compétences en matière d'industrie, de technologie et de recherche et le réseau de centres nationaux de coordination (Journal officiel de l'UE, 8.06.2021 L 202).

Les CETC sont donc priées d'enregistrer [le demandeur XXX].

Une copie de ces informations sera envoyée au demandeur XXX.

ANNEXE 3 – Article 136 du règlement financier de l'UE[5]

L'article 136 du règlement financier prévoit les situations d'exclusion suivantes :

(a) la personne ou l'organisation fait faillite, fait l'objet d'une procédure d'insolvabilité ou de liquidation, ses actifs sont gérés par un syndic ou une juridiction, fait l'objet d'un concordat préventif, ses activités sont suspendues ou se trouve dans une situation similaire résultant d'une procédure similaire en vertu du droit de l'Union ou du droit national ;
b) il a été établi, par un jugement définitif ou une décision administrative, que la personne ou l'entité ne respecte pas ses obligations relatives au paiement des impôts ou des cotisations de sécurité sociale conformément au droit applicable ;
c) il a été établi, par un jugement définitif ou une décision administrative définitive, que la personne ou l'entité a commis une faute professionnelle grave en contrevenant aux lois ou règlements applicables ou aux normes déontologiques de la profession à laquelle elle appartient, ou en se livrant à une faute ayant une incidence sur sa crédibilité professionnelle, lorsqu'un tel comportement indique une intention fautive ou une négligence grave, y compris, en particulier, l'un des éléments suivants :

(i) faire de fausses déclarations frauduleuses ou par négligence concernant les informations nécessaires pour vérifier l'absence de motifs d'exclusion ou le respect des critères d'éligibilité ou de sélection ou pour mettre en œuvre l'engagement juridique ;

ii) conclure un accord avec d'autres personnes ou entités dans le but de fausser la concurrence ;

iii) violation des droits de propriété intellectuelle ;

iv) tenter d'influencer la prise de décision de l'ordonnateur compétent au cours de la procédure de passation de marché ;

c) en tentant d'obtenir des informations confidentielles susceptibles de lui conférer des avantages indus dans le cadre de la procédure d'attribution ;

d), il a été établi de façon définitive que la personne ou l'entité est coupable de l'un ou l'autre des actes suivants :

i) la fraude, au sens de l'article 3 de la directive (UE) 2017/1371 du Parlement européen et du Conseil (44) et de l'article 1er de la convention relative à la protection des intérêts financiers des Communautés européennes, établie par l'acte du Conseil du 26 juillet 1995 (45) ;

ii) la corruption, au sens de l'article 4, paragraphe 2, de la directive (UE) 2017/1371 ou la

[5] Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) n° 1296/2013, (UE) n° 1301/2013, (UE) n° 1303/2013, (UE) n° 1304/2013, (UE) n° 1309/2013, (UE) n° 1316/2013, (UE) n° 223/2014, (UE) n° 283/2014 et la décision n° 541/2014/UE et abrogeant le règlement (UE, Euratom) n° 966/2012 - PE/13/2018/REV/1 - https://eur-lex.europa.eu/eli/reg/2018/1046/oj/eng

corruption active au sens de l'article 3 de la convention relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des États membres de l'Union européenne, établie par l'acte du Conseil du 26 mai 1997 (46), ou le comportement visé à l'article 2, paragraphe 1, de la décision-cadre 2003/568/JAI du Conseil (47), ou la corruption telle que définie dans d'autres lois applicables ;

iii) les comportements liés à une organisation criminelle visés à l'article 2 de la décision-cadre 2008/841/JAI du Conseil (48) ;

iv) le blanchiment de capitaux ou le financement du terrorisme au sens de l'article 1er, paragraphes 3, 4 et 5, de la directive (UE) 2015/849 du Parlement européen et du Conseil (49) ;

v) les infractions terroristes ou les infractions liées à des activités terroristes, telles que définies respectivement aux articles 1er et 3 de la décision-cadre 2002/475/JAI du Conseil (50), ou l'incitation, la complicité ou la tentative de commettre de telles infractions, telles que visées à l'article 4 de ladite décision ;

vi) le travail des enfants ou d'autres infractions liées à la traite des êtres humains visées à l'article 2 de la directive 2011/36/UE du Parlement européen et du Conseil (51) ;

e), la personne ou l'entité a démontré des manquements importants dans le respect d'obligations clés dans l'exécution d'un engagement juridique financé par le budget qui a :

(i), a conduit à la résiliation anticipée d'un engagement juridique ;

(ii) a donné lieu à des dommages-intérêts liquidés ou à d'autres pénalités contractuelles ; ou

iii) ont été découverts par un ordonnateur, l'OLAF ou la Cour des comptes à la suite de contrôles, d'audits ou d'enquêtes ;

f) il a été établi, par un jugement définitif ou une décision administrative définitive, que la personne ou l'entité a commis une irrégularité au sens de l'article 1er, paragraphe 2, du règlement (CE, Euratom) no 2988/95 du Conseil (52) ;

g) il a été établi, par un jugement définitif ou une décision administrative, que la personne ou l'entité a créé une entité dans une autre juridiction dans l'intention de se soustraire à des obligations fiscales, sociales ou autres obligations juridiques dans la juridiction de son siège statutaire, de son administration centrale ou de son principal établissement ;

h), il a été établi, par un jugement définitif ou une décision administrative définitive, qu'une entité a été créée avec l'intention visée au point g).