CONVENTION DE CONTRIBUTION FINANCIERE ET MANDAT DE MISSION PUBLIQUE PLURIANNUELLE 2021 – 2025

Entre L'État du Grand-Duché de Luxembourg, représenté par :

- *Monsieur Franz Fayot, Ministre de l'Économie, demeurant professionnellement à L-2449 Luxembourg, 19-21 boulevard Royal,*

ci-après dénommé « l'État » ;

d'une part, et

le groupement d'intérêt économique « Security Made in Lëtzebuerg » (en abrégé SECURITYMADEIN.LU), représenté par

- *Monsieur François Thill, Président, demeurant professionnellement à L-2449 Luxembourg, 19-21 boulevard Royal,*
- *Monsieur Carlo Gambucci, Vice-Président, demeurant professionnellement à L-5326 Contern, 11, rue Edmond Reuter,*

ci-après dénommé « le Groupement » d'autre part.

Dans le cadre de la *stratégie nationale en matière de cybersécurité*[1], la « *Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg* »[2], l'« *Intelligence artificielle: une vision stratégique pour le Luxembourg* »[3] ainsi que les efforts de *promotion et de soutien au développement de la société digitale* du Grand-Duché de Luxembourg,

- Vu le contrat constitutif du Groupement, ci-après dénommé « le Contrat Constitutif », constitué par acte sous seing privé en date du 05 mai 2010 entre le ministère de l'Économie et du Commerce extérieur, le ministère de l'Éducation nationale et de la Formation professionnelle, le ministère de la Famille et de l'Intégration, le Syndicat Intercommunal de Gestion Informatique, et le Syndicat intercommunal à vocation multiple des Villes et des Communes Luxembourgeoises ;
- Vu l'article 8 du Contrat Constitutif, stipulant que les contributions des membres du Groupement au financement du budget annuel sont à supporter par l'ensemble des membres seront réalisés au prorata de leurs engagements financiers initiaux tels qu'indiqués lors de la signature du Contrat Constitutif ;
- Considérant la volonté de l'État, inscrite en l'article 3 du Contrat Constitutif, d'une part de soutenir les communes, citoyens et entreprises du Luxembourg afin d'accroître le niveau de qualité et de sécurité de leurs systèmes et réseaux d'information et de communication, et d'autre part de soutenir la sécurité informatique des services et administrations gouvernementaux (ci-après collectivement dénommés « les Objectifs ») ;

---

[1] https://hcpn.gouvernement.lu/fr/publications/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3.html

[2] https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-economie/the-data-driven-innovation-strategy.pdf

[3] https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-digitalisation/intelligence-artificielle-une-vision-strategique-pour-le-luxembourg.pdf

- Vu les attributions du Ministère de l'Économie [4] dans les domaines du commerce électronique, de l'archivage électronique, de la signature électronique, de la sécurité de l'information, comme de la sensibilisation aux risques, menaces et vulnérabilités du secteur privé ;
- Vu loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 (NIS Directive) du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne, dis « loi NIS »[5], en particulier vu le rôle de CIRCL, un département du Groupement ;
- Considérant les rôles spécifiques du Groupement (via son département CIRCL) dans le cadre du Plan d'Intervention d'Urgence « Cyber » (PIU cyber), défini par les autorités en cas de faille technique ou d'attaque d'envergure contre les systèmes d'information du secteur public et/ou du secteur privé[6]
- Considérant le soutien apporté par l'État du Grand-Duché de Luxembourg, en particulier l'article 41.011 du Budget de l'État, portant le libellé : « Participation financière aux frais de fonctionnement du Groupement d'Intérêt Économique "Security made in Lëtzebuerg", le SIGI et le SYVICOL (ci-après dénommés "les Membres") au Groupement dans la mise en œuvre des Objectifs ;
- Considérant les conventions de contribution précédentes, signées les 13/06/2014 et 18/12/2014, entre le Groupement et le Ministère de l'Économie ;

il est convenu ce qui suit :

ARTICLE 1 – OBJET

L'objet de la présente convention de contribution financière et mandat de mission publique pluriannuelle 2021-2025 (ci-après dénommée « la Convention ») consiste à préciser le mandat de mission publique dans le cadre des Objectifs du Groupement tels qu'octroyés par l'État et les modalités et montants de la contribution financière pluriannuelle de l'État (ci-après dénommée « la Contribution ») en vue de la participation aux frais de fonctionnement du Groupement en application du Contrat Constitutif pour les années 2021 à 2025 incluses, en particulier en vue d'exécuter le mandat de mission publique définit ci-après.

ARTICLE 2 – DUREE

La Convention est conclue avec effet rétroactif au 1er janvier 2021 pour une durée de 5 années (60 mois). Elle cessera donc ses effets de plein droit le 31 décembre 2025.

ARTICLE 3 – IDENTIFICATION

Le Groupement étant un des acteurs majeurs de la cybersécurité nationale[7] et vu son rôle en relation avec le développement économique du secteur de la cybersécurité, ainsi que les efforts y relatifs que le Groupement a réalisés depuis sa création, il sera identifié, connu et promu dès à présent, comme

« Agence de Cybersécurité pour les Communes et l'Économie Luxembourgeoise » (FR)

« Cybersecurity Agency for the Luxembourg Economy and Municipalities » (EN)

---

[4] http://legilux.public.lu/eli/etat/leg/agd/2018/12/05/a1099/jo
[5] http://legilux.public.lu/eli/etat/leg/loi/2019/05/28/a372/jo
[6] https://www.infocrise.lu/fr/cyber-acteurs-organes-gestion
[7] Le Groupement est membre du « comité interministériel de coordination en matière de cyberprévention et de cybersécurité », cf. pages 11 à 13 de la stratégie nationale en matière de cybersécurité III (https://hcpn.gouvernement.lu/fr/publications/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3.html)

ARTICLE 4 – MANDAT DE MISSION PUBLIQUE

L'État du Grand-Duché de Luxembourg mandate le Groupement SECURITYMADEIN.LU avec les missions publiques suivantes (voir le détail à l'annexe 1) et au bénéfice du secteur privé, des communes et des entités non-gouvernementales du Luxembourg :

1. De fournir des services et outils de sensibilisation, des méthodes et outils de gouvernance et des méthodes, outils, scénarios et métriques pour la gestion des risques « cyber », favorisant la démocratisation et la diffusion des bonnes pratiques en sécurité de l'information, gérés par son département CASES (« Cyberworld Awareness and Security Enhancement Services » [8]). Dans le cadre de la réglementation européenne « Cybersecurity Act »[9], CASES assurera un service de certification dédié au secteur privé, ceci en vue d'améliorer la maturité du tissu économique luxembourgeois voire européen,

   ci-après « mandat CASES » ;

2. D'agir comme centre de collecte, d'agrégation et de partage d'informations sur les menaces, vulnérabilités et mesures de protection en fournissant les outils, le leadership communautaire, les meilleures pratiques, les normes d'échange, les ontologies et taxonomies ainsi que les données, pour un large éventail de communautés et de secteurs. Ce centre, géré par le département CIRCL (« Computer Incident Response Center Luxembourg »[10]), est le point de contact fiable et de confiance pour tous les utilisateurs, entreprises et organisations basés au Luxembourg en cas d'attaques ou d'incidents informatiques et point de contact pour la notification d'incidents dans le cadre de la directive « NIS »,

   ci-après « mandat CIRCL » ;

3. D'accompagner au travers de son département C3 (« Cybersecurity Competence Center »[11]), le développement à long-terme des compétences et le renforcement des capacités individuelles et collectives, en matière de cybersécurité, de tous les acteurs du tissu économique luxembourgeois, de mettre en place et de gérer un « data space » cybersécurité mettant à disposition des informations pertinentes selon une ontologie et une taxonomie promouvant la collaboration et la création de modèles d'affaires. C3 met en place un service de due diligence pour l'évaluation des produits, services et processus des « start-ups ».
   Le centre assurera également le rôle de centre national dans le cadre de la future réglementation européenne « European Cybersecurity Competence Centre »[12],

   ci-après « mandat C3 » ;

[8] https://www.cases.lu/
[9] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[10] https://www.circl.lu/
[11] https://c-3.lu/
[12] Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres - https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54252

4. De fédérer l'écosystème cybersécurité luxembourgeois, et le promouvoir par le biais de la marque nationale « CYBERSECURITY LUXEMBOURG »[13], partie intégrante de la boîte à outils pour valoriser l'image et structurer la promotion du Luxembourg[14] dans le domaine de la cybersécurité,

   ci-après « mandat CYBERLUX ».

ARTICLE 5 – GOUVERNANCE

La mise en œuvre des moyens permettant d'exécuter les mandats de mission publique ci-avant (art. 4) suit le modèle de gouvernance comme suit :

I. Plan d'action et budget annuel, par mandat de mission publique (janvier) ;
II. Établissement d'un état des lieux de la cybersécurité de l'économie luxembourgeoise (biannuel : mars et septembre) ;
III. Budget prévisionnel des dépenses et recettes pour les années suivantes (avril) ;
IV. Rapport et bilan des activités de l'année précédente (mai) ;
V. Revue biannuelle des résultats du plan d'action (juin et novembre) ;

ARTICLE 6 – FINANCEMENT

En application des dispositions et modalités indiquées dans l'Article 8 du Contrat Constitutif et pour la mise en œuvre des missions publiques (art. 4), l'État s'engage à accorder au Groupement une Contribution équivalente au budget pluriannuel prévisionnel pour les 5 prochaines années (ci-après dénommé « le Budget », voir aussi les annexes 2 et 3) ainsi que les postes en termes de ressources humaines (ci-après dénommé « le Plan RH », voir aussi l'annexe 3) y associées et nécessaire à l'exécution de la présente Convention.

Le Budget ainsi que le Plan RH peuvent être revus d'année en année, et ils sont entendus comme arrêtés par le Collège de Gérance du Groupement au 1er janvier de l'année concernée, et établis sur la base du Plan d'action de mise en œuvre des missions publiques du Groupement (annexe 1).

Cette Contribution n'exclut pas l'attribution de moyens financiers publics supplémentaires, en provenance de tout autre crédit budgétaire éligible (national, européen ou de provenance internationale). De même, il est entendu entre les Parties que cette Contribution ne sera pas impactée par les éventuels revenus financiers de SECURITYMADEIN.LU réalisés dans le cadre d'opérations commerciales tierces, ou de partenariats commerciaux.

CYBERSECURITY LUXEMBOURG

[13]

[14] https://luxembourg.public.lu/fr/boite-a-outils.html

Les demandes de versement de cette Contribution seront réalisées par SECURITYMADEIN.LU en quatre (4) tranches selon les modalités suivantes :

Date	***Pourcentage de la Contribution***
Avant le 15 janvier de l'année en cours	*30%*
Avant le 15 avril de l'année en cours	*30%*
Avant le 15 juillet de l'année en cours	*20%*
Avant le 15 octobre de l'année en cours	*20%*

ARTICLE 7 – ENGAGEMENTS DU GROUPEMENT

Le Groupement s'engage à

- mettre en œuvre les mandats de mission publique (art. 4.),
- suivre le modèle de gouvernance prévu à l'article 5,
- remettre à l'État aux dates convenues les documents et rapports identifiés aux articles 5 et 6.

ARTICLE 8 – RESPONSABILITES

Chaque partie contractante exonère l'autre partie de toute responsabilité civile du fait des dommages subis par elle-même ou par son personnel résultant de l'exécution de la Convention, dans la mesure où ces dommages ne sont pas dus à une faute grave ou intentionnelle de l'autre partie contractante ou de son personnel.

L'État ne peut être tenu responsable d'actes ou de manquements commis par SECURITYMADEIN.LU lors de l'exécution de la présente Convention.

ARTICLE 9 – INEXECUTION, RETARDS OU DEFAILLANCES

SECURITYMADEIN.LU et l'État s'engagent à se signaler réciproquement et sans délai, en se fournissant toutes précisions utiles, tout événement susceptible de porter préjudice à l'exécution de la Convention. Dans ce cas, les Parties fixent les mesures à prendre d'un commun accord.

ARTICLE 10 – CONTROLE

SECURITYMADEIN.LU conservera, pendant une période de 10 ans après l'échéance finale de la période couverte par la Convention, l'original ou, dans des cas exceptionnels dûment justifiés, les copies certifiées conformes de l'original de tous les documents concernant la Convention ou son exécution, en particulier les éléments identifiés aux articles 5 et 6. Durant l'exécution d'audits dans le cadre de la Convention, ces documents seront mis sur demande à la disposition des personnes chargées de ces audits.

ARTICLE 11 – MODIFICATIONS DE LA CONVENTION

Les dispositions de la Convention pourront être modifiées que d'un commun accord entre SECURITYMADEIN.LU et l'État, moyennant un avenant écrit.

ARTICLE 12 – DROIT APPLICABLE ET JURIDICTION COMPETENTE

La Convention est soumise au droit luxembourgeois et tout litige en relation avec la Convention est de la compétence exclusive des tribunaux de l'arrondissement judiciaire de Luxembourg, Grand-Duché de Luxembourg.

Fait à Luxembourg, le 08. FEB. 2021 en autant d'exemplaires que de parties.

Pour l'État du Grand-Duché de Luxembourg,

Monsieur Franz Fayot,
Ministre de l'Économie

Pour « Security Made in Lëtzebuerg » g.i.e.

Monsieur François Thill,
Président

Monsieur Carlo Gambucci,
Vice-Président

ANNEXE 1 – DETAILS DES ACTIONS ET ACTIVITES DES MANDATS DE MISSION PUBLIQUE DE SECURITYMADEIN.LU

ANNEXE 1.1 – ACTIONS ET ACTIVITES DU « MANDAT CASES »

Dans le cadre du mandat de mission publique, dit « CASES », et selon le descriptif précité, à savoir :

> *Fournir des services et outils de sensibilisation, des méthodes et outils de gouvernance et des méthodes, outils, scénarios et métriques pour la gestion des risques « cyber », favorisant la démocratisation et la diffusion des bonnes pratiques en sécurité de l'information, gérés par son département CASES. Dans le cadre de la réglementation européenne « Cybersecurity Act », CASES assurera un service de certification dédié au secteur privé, ceci en vue d'améliorer la maturité du tissu économique luxembourgeois voire européen;*

les actions, activités, outils et plateformes, y associés sont décrites ci-dessous[15] :

I. Sensibilisation et dissémination de bonnes pratiques de la sécurité de l'information
   - ⇒ www.cases.lu
   - ⇒ trustbox.cases.lu
   - ⇒ Training et train-the-trainer

II. Soutien d'organismes, d'entreprises, et en particulier de PMEs, dans leurs « premier pas » et démarches organisationnelles en sécurité de l'information
   - ⇒ Fit4Cybersecurity et autres
   - ⇒ Diagnostic CASES

III. Modélisation de risques « cyber » suivant les référentiels principaux en sécurité de l'information. Soutien d'organismes dans la modélisation de leurs processus métier en un modèle risques
   - ⇒ MONARC

IV. Mise à disposition de ressources digitales, de documentations, de modèles et d'indicateurs de risques à destination de tout acteur en gouvernance cybersécurité et en gestion de risques de l'information
   - ⇒ MOSP, Informed governance
   - ⇒ Contribution au « data space » cybersécurité géré par le C3

V. Facilitation par différents moyens (e.g. mise en place d'un service de certification dans le cadre de la réglementation européenne « Cybersecurity Act ») l'amélioration de la maturité du tissu économique luxembourgeois voire européen.

[15] La liste d'actions, activités, outils et plateformes est non exhaustive, mais évolutive selon les besoins de l'actualité ou suivant des demandes spécifiques du Ministère de l'Économie, ceux-ci garantissant la continuité des activités, outils, plateformes et services existants.

ANNEXE 1.2 – ACTIONS ET ACTIVITES DU « MANDAT CIRCL »

Dans le cadre du mandat de mission publique, dit « CIRCL », et selon le descriptif précité, à savoir :

> *Agir comme centre de collecte, d'agrégation et de partage d'informations sur les menaces, vulnérabilités et mesures de protection en fournissant les outils, le leadership communautaire, les meilleures pratiques, les normes d'échange, les ontologies et taxonomies ainsi que les données, pour un large éventail de communautés et de secteurs. Ce centre, géré par le département CIRCL, est le point de contact fiable et de confiance pour tous les utilisateurs, entreprises et organisations basés au Luxembourg en cas d'attaques ou d'incidents informatiques et point de contact pour la notification d'incidents dans le cadre de la directive « NIS »;*

les actions, activités, outils et plateformes, y associées sont décrites ci-dessous[16] :

I. Coordination et gestion d'incidents informatiques au bénéfice de tous les acteurs de l'économie luxembourgeoise, y incluent la coopération avec les spécialistes nationaux et internationaux impliqués ;
   - ⇒ www.circl.lu/report/
   - ⇒ www.circl.lu/pub/responsible-vulnerability-disclosure/

II. Collecte et recherche d'informations sur les menaces et vulnérabilités et d'indicateurs d'attaques sur les systèmes luxembourgeois
   - ⇒ AIL
   - ⇒ D4
   - ⇒ URLABUSE

III. Partage et mise à disposition d'informations sur les cybermenaces (statistiques, « facts and figures », « situational awareness ») à destination des équipes opérationnelles en sécurité informatique ;
   - ⇒ MISP
   - ⇒ www.circl.lu/opendata
   - ⇒ CVE
   - ⇒ X-ISAC

IV. Soutien et mise à disposition d'outils et de services en ligne à la communauté de sécurité opérationnelle luxembourgeoise et européenne
   - ⇒ DMA
   - ⇒ BGP Ranking
   - ⇒ Passive DNS/SSL

V. Participation aux groupes de travail européens, en particulier dans le cadre de la directive européenne « NIS », et les fora internationaux du domaine des CSIRTs, « digital forensics » et sur le sujet de la réponse sur incidents.
   - ⇒ CSIRT network
   - ⇒ TF-CSIRT
   - ⇒ FIRST

[16] La liste d'actions, activités, outils et plateformes est non exhaustive, mais évolutive selon les besoins de l'actualité ou suivant des demandes spécifiques du Ministère de l'Économie, ceux-ci garantissant la continuité des activités, outils, plateformes et services existants.

ANNEXE 1.3 – ACTIONS ET ACTIVITES DU « MANDAT C3 »

Dans le cadre du mandat de mission publique, dit « C3 », et selon le descriptif précité, à savoir :

> *Accompagner, au travers de son département C3, le développement à long-terme des compétences et le renforcement des capacités individuelles et collectives, en matière de cybersécurité, de tous les acteurs du tissu économique luxembourgeois, de mettre en place et de gérer un « data space » cybersécurité mettant à disposition des informations pertinentes selon une ontologie et une taxonomie promouvant la collaboration et la création de modèles d'affaires. C3 met en place un service de due diligence pour l'évaluation des produits, services et processus des « start-ups ». Le centre assurera également le rôle de centre national dans le cadre de la future réglementation européenne « European Cybersecurity Competence Centre »;*

les actions, activités, outils et plateformes, y associées sont décrites ci-dessous[17] :

I. Élaboration et mise à disposition d'un cadre de référence (« framework ») en « cybersecurity competence & capacity building », permettant aux acteurs économiques Luxembourgeois de définir une stratégie et de développer leurs compétences internes en cybersécurité (e.g. rôles-types, descriptions standardisées des connaissances (« savoirs ») et des savoirs-faire...)
   ⇒ c3.lu

II. Accompagnement et transfert de connaissance en cybersécurité à tout organisme luxembourgeois, ceci en étroite collaboration avec l'expertise et les spécialistes du marché
   ⇒ training.c3.lu (plateforme de « guidance » à la sélection de partenaires correspondants aux besoins spécifiques des demandeurs)
   ⇒ ROOM#42 (renforcer et favoriser la formation basée sur l'expérience)

III. Mise à disposition de plateformes, services et outils, permettant aux organisations de tester facilement la robustesse et la résilience aux cybermenaces, en étroite collaboration avec l'expertise et les spécialistes du marché
   ⇒ testing.c3.lu (plateforme multi-modale permettant l'identification des points de faiblesse des organisations dans le but de mettre à jour les compétences individuelles et collectives manquantes ou insuffisantes)

IV. Mise en place et gestion d'un « data space » cybersécurité mettant à disposition des informations pertinentes selon une ontologie et une taxonomie promouvant la collaboration et la création de modèles d'affaires, capitalisant en particulier sur les informations et données de CASES, CIRCL et CYBERLUX.

V. Élaboration et distribution de rapports, bulletins et/ou analyses des menaces et vulnérabilités particulièrement touchant le Luxembourg afin de permettre aux acteurs d'allouer plus efficacement leurs ressources en matière de cybersécurité
   ⇒ observatory.c3.lu (utilisant d'un maximum de sources de données disponibles ; diffusion en 2 formats : « human readable » et « machine readable »)

VI. Mise en place des services et outils nécessaires à l'établissement du centre de coordination national dans le cadre de la future réglementation européenne « European Cybersecurity Competence Centre ».

VII. Soutien à la maturation de l'écosystème en matière de compétences collectives et individuelles

[17] La liste d'actions, activités, outils et plateformes est non exhaustive, mais évolutive selon les besoins de l'actualité ou suivant des demandes spécifiques du Ministère de l'Économie, ceux-ci garantissant la continuité des activités, outils, plateformes et services existants.

⇒ LCSC (plateforme de challenges, afin de permettre aux résidents de s'auto-évaluer et s'auto-former, et de repérer des (jeunes) talents, pouvant notamment rejoindre l'équipe nationale en cybersécurité « Lëtz Cybersecurity Team »)

ANNEXE 1.4 – ACTIONS ET ACTIVITES DU « MANDAT CYBERLUX »

Dans le cadre du mandat de mission publique, dit « CYBERLUX », et selon le descriptif précité, à savoir :

> *Fédérer l'écosystème cybersécurité luxembourgeois, et le promouvoir par le biais de la marque nationale « CYBERSECURITY LUXEMBOURG », partie intégrante de la boîte à outils pour valoriser l'image et structurer la promotion du Luxembourg dans le domaine de la cybersécurité ;*

Les actions, activités, outils et plateformes, y associées sont décrites ci-dessous[18] :

I. Fédérer l'écosystème cybersécurité luxembourgeois, ainsi que la communauté des professionnels, en favorisant l'échange entre pairs, le partage de « lessons learned » et la dissémination de bonnes pratiques
   - ⇒ cybersecurity.lu
   - ⇒ Cybersecurity Breakfast Series
   - ⇒ Cybersecurity Week
   - ⇒ Ecosystem Newsletter

II. Promouvoir l'écosystème et du marché luxembourgeois en cybersécurité au niveau européen et international, faire le suivi des prospects, effectuer des contrôles de type de diligence technique
   - ⇒ cybersecurity-luxembourg.lu
   - ⇒ foires et conférences (FIC, it-sa, Cybertech...)

III. Accompagner des efforts d'innovation et de recherche en cybersécurité, promouvoir l'établissement de « startups » et autres projets innovants en matière de cybersécurité, et ceci en étroite collaboration avec le « National Cybersecurity Competence Centre », opéré par le C3
   - ⇒ Cybersecurity Startup Pathway
   - ⇒ Liens avec SnT, Startup Luxembourg, House of Startups...

IV. Renforcer des collaborations et développer des projets communs dans la Grande Région franco-germano-luxembourgeoise, et sur un niveau européen
   - ⇒ ENISA
   - ⇒ ECSO
   - ⇒ EU Cyber Valley
   - ⇒ ...

[18] La liste d'actions, activités, outils et plateformes est non exhaustive, mais évolutive selon les besoins de l'actualité ou suivant des demandes spécifiques du Ministère de l'Économie, ceux-ci garantissant la continuité des activités, outils, plateformes et services existants.