CONSEIL D'ADMINISTRATION

Séance du mercredi 20 mai 2026

Délibération n° 2026-42
Conventions

Le Conseil d'Administration de l'université des Antilles, dans sa séance du 20 mai 2026, sous la présidence de Monsieur le Professeur Michel GEOFFROY, Président de l'université des Antilles,

Vu le livre VII du Code de l'Education,
Vu les statuts de l'université des Antilles,

a délibéré

Après s'être assuré du quorum, suite à la présentation et aux débats qui s'en sont suivis, le Président de l'université demande aux membres du Conseil d'Administrationde procéder au vote :

Il s'agit d'approuver les conventions suivantes :

- *Accord de consortium - Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)*
- *Avenant n°1 à la convention de reversement de fonds UA/ ACCYB*

Résultat du vote :

Membres en exercice	**30**
Membres présents ou représentés	28
Membres n'ayant pas pris part au vote	0
Contre	0
Abstention	0
Pour	**28**

Les conventions, telles que jointes en annexe, sont approuvées à l'unanimité des membres présents et représentés du Conseil d'Administration.

Pour extrait certifié conforme,
Fait à Pointe–à-Pitre, le 21 mai 2026

Le Président de l'université des Antilles

Pr. Michel GEOFFROY

Modalités de recours contre la présente délibération :
En application de l'article R.421-1 du code de justice administrative, le tribunal administratif peut être saisi par voie de recours formé contre la présente délibération, et ce, dans les deux mois à partir du jour de sa publication et de sa transmission au recteur, en cas de délibération à caractère réglementaire. Le tribunal administratif peut être saisi par l'application informatique « Télérecours Citoyens » accessible par le site internet www.telerecours.fr

Université des Antilles
Siège - Administration générale
Campus de Fouillole - BP 250 - 97157 Pointe-à-Pitre cedex - Tél. +0590 (0) 590 483 030
www.univ-antilles.fr

ACCORD DE CONSORTIUM

Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)

ENTRE LES SOUSSIGNES

L'Université des Antilles
Etablissement public à caractère scientifique, culturel et professionnel (EPSCP)
Référencée sous le numéro SIRET 199 715 855 00011
Située au Campus de Fouillole, BP 250, 97175 Pointe-à-Pitre, Guadeloupe
Représentée par son Président, Pr. Michel GEOFFROY

Ci-après dénommée par « UA » ou « le Chef de file »

D'une part

ET

Lycée des Droits de l'Homme – GRETA-CFA de la Guadeloupe,
Etablissement Public - Code APE 8559A
Référencé sous le numéro SIRET : 199 710 088 00022
Situé Pointe à Bacchus - BP 548 – 97170 Petit-Bourg,
Représenté par sa CESUP Elisabeth LEPIERRE

Ci-après dénommée par « le GRETA de la Guadeloupe » ou « le Partenaire »

D'autre part

ET

Rectorat de la Région Académique de la Guadeloupe,
Autre établissement Public à but non lucratif - Code APE 8412z
Référencé sous le numéro SIRET : 179 714 303 00238
Situé à Parc d'activités de la Providence – Zac de Dothémare – 97139 Les Abymes
Représenté par son Recteur de région académique, Gabriele FIONI

ci-après dénommée par «le rectorat de l'académie Guadeloupe » ou « l'Etablissement partenaire »

D'autre part

ET

Association Agence Caribéenne pour la Cybersécurité,
Association enregistrée au registre des associations W9G1011279 au Code APE 94.99Z
Référencé sous le numéro SIRET : 918 714 890 00012
Situé 189 rue Victor MAMADO 97128 GOYAVE
Représenté par son Président, Steven COCKS,

ci-après dénommée par « ACCYB » ou « l'Etablissement partenaire »

D'autre part

[1] Le contexte de référence est celui de la réglementation européenne en matière de recherche, développement et innovation (dit RDI), plus spécifiquement ici l'Encadrement des aides d'Etat à la RDI 2014/C 198/01, articles 28b 28c 28d (présomptions d'absence d'aide indirecte).

ET

ORANGE ANTILLES-GUYANE,
Enterprise de télécommunications filaires Code APE 6110Z
Référencé sous le numéro SIRET : 380 129 866 48625
Situé Imm Simpex Zi De Jarry 7 3 lot Moudong Sud, 97122 Baie-Mahault
Représenté par sa directrice, Chantal MAURICE,

ci-après dénommée par « ORANGE » ou « l'Etablissement partenaire »

D'autre part

ET

Rectorat de l'Académie de la Martinique,
Autre établissement Public à but non lucratif - Code APE 8412z
Référencé sous le numéro SIRET : 179 724 307 00030
Situé à Les Hauts de Terreville – 97279 Schoelcher Cedex,
Représenté par sa Rectrice de région académique, Nathalie MONS

ci-après dénommée par «le Rectorat de l'académie de Martinique » ou « l'Etablissement partenaire »

D'autre part

ET

GIP-FCIP de l'académie de Martinique
Autre établissement Public à but non lucratif - Code APE 8559A
Référencé sous le numéro SIRET : 189 729 056 00011
Situé à 4 rue du Père Delawarde – Plateau Desrochers – 97200 Fort-de-France,
Représenté par son directeur, Olivier CHEVILLARD,

ci-après dénommée par «le GIP-FCIP » ou « l'Etablissement partenaire »

Ci-dessous dénommées collectivement les Parties ou les Partenaires ou individuellement la Partie ou le Partenaire.

PREAMBULE

Les Partenaires ont mis en place un projet collaboratif dénommé **CyberEDAntilles**, destiné à réaliser conjointement des travaux dans le cadre de l'action « Compétences et métiers d'avenir », financée notamment par l'Agence nationale de la recherche (ANR).
Les objectifs poursuivis par les Partenaires dans le cadre du Projet sont décrits dans l'annexe « Description du Projet ».
Il est précisé que l'Université des Antilles bénéficie d'un soutien financier au titre des fonds publics attribués par l'ANR dans le cadre de l'action « Compétences et métiers d'avenir ». Ces financements peuvent être reversés aux autres Partenaires dans les conditions prévues par des conventions spécifiques.
Les Partenaires souhaitent organiser leurs relations dans le cadre de la mise en œuvre du Projet, conformément aux règles applicables aux projets collaboratifs de recherche et d'innovation.
En conséquence, il a été convenu ce qui suit.

ARTICLE 1 – DEFINITIONS

Au sens du présent Contrat, les termes suivants auront la signification ci-après :

Connaissances Propres : Désignent les connaissances, informations, savoir-faire, secrets de fabrication, données, logiciels, méthodes et droits de propriété intellectuelle détenus par un Partenaire avant l'entrée en vigueur du présent Contrat ou développés en dehors du Projet.

Résultats : Désignent l'ensemble des connaissances, données, méthodes, logiciels, prototypes, inventions et savoir-faire obtenus dans le cadre de la réalisation du Projet.

Partenaire : Désigne toute entité signataire du présent Contrat et participant à la réalisation du Projet.

Coordinateur : Désigne le Partenaire chargé d'assurer la coordination scientifique, technique et administrative du Projet.

Projet : Désigne le projet collaboratif CyberEDAntilles tel que décrit dans l'annexe « Description du Projet ».

ARTICLE 2 – OBJET

Le présent Contrat a pour objet d'organiser les relations entre les Partenaires dans le cadre de la réalisation du Projet, et notamment de :

- définir leurs droits et obligations respectifs ;
- organiser la gouvernance du consortium ;
- déterminer les modalités de gestion et de suivi des Résultats ;
- fixer les règles relatives à la propriété intellectuelle des Connaissances Propres et des Résultats ;
- préciser les conditions de communication et de diffusion des résultats du Projet.

ARTICLE 3 – DUREE

Le présent Contrat entre en vigueur rétroactivement à la **Date d'Effet**, sous réserve de sa signature par l'ensemble des Partenaires.
Il est conclu pour une durée courant **du 1er janvier 2025 au 30 juin 2030**.
La durée du Contrat pourra être prolongée si le Projet est lui-même prolongé par le financeur, par voie d'avenant signé par les Partenaires.
Certaines clauses, notamment celles relatives à la propriété intellectuelle, à la confidentialité et aux publications, continueront à produire leurs effets après l'expiration du Contrat pour la durée nécessaire à leur application.

ARTICLE 4 – GOUVERNANCE DU CONSORTIUM

La gouvernance du consortium repose sur les instances suivantes :

- un **Coordinateur** ;
- un **Comité de Pilotage** ;
- un **Conseil pédagogique et stratégique** ;
- un **Comité opérationnel**.

4.1 COORDINATEUR

L'**Université des Antilles** est désignée Coordinateur du Projet. À la date de signature du présent Contrat, le représentant désigné pour assurer cette fonction est : **Pr. Erick STATTNER**

Le Coordinateur assure notamment :

- la coordination scientifique et technique du Projet ;
- la relation avec l'ANR ;
- la circulation de l'information entre les Partenaires ;
- l'organisation des réunions du Comité de Pilotage ;
- le suivi de l'avancement des travaux.

Le Coordinateur ne peut engager les autres Partenaires sans leur accord préalable.

4.2 COMITE DE PILOTAGE

COMPOSITION

Le Comité de Pilotage est composé d'un représentant de chaque Partenaire.
La liste des représentants est annexée au présent Contrat.
Le Comité de Pilotage est présidé par le Coordinateur.

REUNIONS

Le Comité de Pilotage se réunit :

- au moins une fois par mois durant la première année du Projet ;
- puis au moins une fois par trimestre.

DECISIONS

Le Comité de Pilotage prend ses décisions à la **majorité qualifiée des trois quarts des membres**, sauf disposition contraire du présent Contrat.

ROLE

Le Comité de Pilotage est notamment chargé :

- de définir les orientations scientifiques et stratégiques du Projet ;
- de suivre l'avancement des travaux ;
- de valider les livrables ;
- de statuer sur l'entrée ou le retrait d'un Partenaire ;
- de veiller au respect des règles de propriété intellectuelle et de confidentialité.

4.3 CONSEIL PEDAGOGIQUE ET STRATEGIQUE

Le Conseil pédagogique et stratégique est composé d'experts et de parties prenantes du Projet.
Il a notamment pour mission :

- d'assurer une veille sur les besoins en compétences ;
- d'évaluer l'évolution des formations ;
- de contribuer à l'analyse d'impact du Projet.

4.4 COMITE OPERATIONNEL

Le comité opérationnel est chargé de la mise en œuvre concrète des travaux du Projet.
Il est composé de représentants désignés par les Partenaires.
Elle se réunit régulièrement afin d'assurer le suivi opérationnel du Projet.

ARTICLE 5 – ENGAGEMENTS DES PARTENAIRES

Les Partenaires s'engagent à :

- réaliser leur part des travaux conformément à l'annexe « Description du Projet » ;
- coopérer de bonne foi pour atteindre les objectifs du Projet ;
- fournir au Coordinateur les informations nécessaires au suivi du Projet ;
- informer sans délai le Coordinateur de toute difficulté susceptible d'affecter la réalisation du Projet.

Chaque Partenaire met en œuvre les moyens nécessaires à la bonne exécution de ses obligations.
Compte tenu de l'intégration du GIP-FCIP de l'académie de Martinique postérieurement au démarrage du projet, les Partenaires conviennent que les modalités d'organisation de la coopération entre l'académie de Martinique et le GIP-FCIP de l'académie de Martinique sont précisées dans l'annexe 6 « Organisation des relations entre l'académie de Martinique et le GIP-FCIP de l'académie de Martinique ».

ARTICLE 6 – RESPONSABILITE

Chaque Partenaire est responsable de l'exécution de sa Part des Travaux.
La responsabilité d'un Partenaire ne pourra être engagée envers les autres Partenaires qu'au titre des **dommages directs**.
Les dommages indirects, tels que les pertes de bénéfices, de chiffre d'affaires ou d'image, sont expressément exclus.
Chaque Partenaire demeure responsable des dommages causés aux tiers du fait de ses activités.

ARTICLE 7 – FORCE MAJEURE

Aucun Partenaire ne pourra être tenu responsable de la non-exécution de ses obligations résultant d'un cas de force majeure au sens de l'article 1218 du Code civil.
En cas de survenance d'un tel événement, l'exécution des obligations est suspendue pendant la durée de celui-ci.
Si la situation de force majeure se prolonge au-delà de deux mois, le Contrat pourra être résilié par toute Partie non affectée.

ARTICLE 8 – MODIFICATION DU CONSORTIUM

L'entrée d'un nouveau Partenaire dans le consortium doit être approuvée par le Comité de Pilotage et formalisée par un avenant au présent Contrat.
Le retrait ou l'exclusion d'un Partenaire est décidé dans les conditions prévues par le Contrat et par la réglementation applicable au financement du Projet.

ARTICLE 9 – PROPRIETE INTELLECTUELLE DES CONNAISSANCES PROPRES

Chaque Partenaire conserve la propriété exclusive de ses Connaissances Propres.
L'utilisation des Connaissances Propres par les autres Partenaires peut être accordée dans les conditions définies par des licences ou accords spécifiques.

ARTICLE 10 – PROPRIETE INTELLECTUELLE DES RESULTATS

10.1 – Propriété des résultats

Les Résultats obtenus dans le cadre du Projet appartiennent au Partenaire qui les a générés.
Chaque Partenaire est titulaire des droits de propriété intellectuelle afférents aux Résultats qu'il a obtenus dans le cadre de la réalisation de sa Part des Travaux.

Il lui appartient notamment d'assurer, le cas échéant, la protection et la gestion des droits de propriété intellectuelle correspondants, dans le respect des dispositions du présent Contrat et des réglementations applicables.

10.2 – Propriété des résultats

Lorsque des Résultats sont obtenus conjointement par plusieurs Partenaires et qu'il n'est pas possible d'attribuer à chacun une contribution distincte et identifiable, ces Résultats sont réputés être des **Résultats Conjoints**.

Les Résultats Conjoints appartiennent conjointement aux Partenaires qui ont contribué à leur obtention.

Les modalités de gestion, de protection, d'exploitation et, le cas échéant, de répartition des coûts afférents aux Résultats Conjoints feront l'objet d'un **accord spécifique entre les Partenaires copropriétaires**, conformément aux dispositions du Code de la propriété intellectuelle.

À défaut d'accord spécifique, chaque copropriétaire pourra exploiter les Résultats Conjoints pour ses besoins propres, sous réserve de ne pas porter atteinte aux droits des autres copropriétaires.

10.3 – Accès aux Résultats pour la réalisation du Projet

Chaque Partenaire accorde aux autres Partenaires un droit d'accès non exclusif et non transférable aux résultats qu'il détient, lorsque cet accès est nécessaire à la réalisation de leurs parts des travaux dans le cadre du Projet.

Cet accès est accordé à titre gratuit pendant la durée du Projet, sauf disposition contraire décidée par le Comité de Pilotage.

Les modalités pratiques d'accès aux résultats pourront être précisées par accord entre les Partenaires concernés.

10.4 – Exploitation des résultats

Chaque Partenaire est libre d'exploiter les Résultats dont il est propriétaire, directement ou par l'intermédiaire de tiers.

Lorsque les Résultats sont détenus conjointement par plusieurs Partenaires, leurs modalités d'exploitation feront l'objet d'un accord spécifique entre les copropriétaires.

Les Partenaires s'engagent à favoriser, dans la mesure du possible, la valorisation et le transfert des Résultats issus du Projet.

10.5 – Protection des résultats

Les Partenaires décident conjointement de l'opportunité de protéger les Résultats susceptibles de faire l'objet d'une protection par un droit de propriété intellectuelle, notamment par brevet, droit d'auteur ou protection des logiciels.

Lorsqu'un Résultat appartient à un seul Partenaire, celui-ci décide seul de la stratégie de protection.

Lorsqu'un Résultat est détenu conjointement par plusieurs Partenaires :

- les décisions relatives au dépôt, à l'extension et au maintien des titres de propriété intellectuelle sont prises d'un commun accord ;
- les frais associés sont répartis entre les copropriétaires selon des modalités définies entre eux.

Les logiciels développés dans le cadre du Projet sont protégés par le droit d'auteur conformément aux dispositions du Code de la propriété intellectuelle.

10.6 – Règlement des conflits de propriété intellectuelle
En cas de désaccord entre les Partenaires concernant la propriété ou l'exploitation d'un Résultat, les Partenaires concernés s'efforcent de trouver une solution amiable.

À défaut d'accord amiable dans un délai raisonnable, la question est soumise au Comité de Pilotage qui émet une recommandation.

Si le différend persiste, les Partenaires peuvent recourir à une procédure de médiation avant toute action judiciaire.

ARTICLE 11 – CONFIDENTIALITE

Les Partenaires s'engagent à préserver la confidentialité des informations échangées dans le cadre du Projet.
Cette obligation de confidentialité s'applique pendant toute la durée du Contrat et pendant **cinq ans après son expiration**.

ARTICLE 12 – PUBLICATIONS ET COMMUNICATIONS

Les publications scientifiques résultant du Projet sont encouragées.
Toute publication relative au Projet doit faire l'objet d'une information préalable des autres Partenaires afin de protéger les informations confidentielles et les droits de propriété intellectuelle.

ARTICLE 13 – SOUS-TRAITANCE

Chaque Partenaire peut recourir à un sous-traitant pour l'exécution d'une partie de ses travaux, sous réserve de l'approbation du Comité de Pilotage.
Le Partenaire concerné demeure responsable des prestations réalisées par son sous-traitant.

ARTICLE 14 – ASSURANCES

Chaque Partenaire déclare être titulaire d'une assurance couvrant sa responsabilité civile professionnelle.

ARTICLE 15 – PROTECTION DES DONNEES PERSONNELLES

Les Partenaires s'engagent à respecter la réglementation applicable en matière de protection des données personnelles, notamment le **Règlement général sur la protection des données (RGPD)**.

ARTICLE 16 – SECURITE DES SYSTEMES D'INFORMATION

Les Partenaires mettent en œuvre les mesures nécessaires pour assurer la sécurité des systèmes d'information utilisés dans le cadre du Projet.

ARTICLE 17 – CONTROLE DES EXPORTATIONS

Les Partenaires s'engagent à respecter les réglementations applicables en matière de contrôle des exportations de technologies et de données.

ARTICLE 18 – INTEGRITE SCIENTIFIQUE ET ETHIQUE

Les activités de recherche sont menées dans le respect des principes d'intégrité scientifique et des règles éthiques applicables.

ARTICLE 19 – RESILIATION

Le Contrat peut être résilié :

- par accord unanime des Partenaires ;
- en cas de manquement grave d'un Partenaire à ses obligations.

ARTICLE 20 – DROIT APPLICABLE ET REGLEMENT DES DIFFERENDS

Le présent Contrat est régi par le **droit français**.
Tout différend relatif à son interprétation ou à son exécution fera l'objet d'une tentative de règlement amiable.
À défaut d'accord amiable, les tribunaux compétents seront saisis.

ARTICLE 21 – ANNEXES

Les annexes suivantes font partie intégrante du présent Contrat :

- Annexe 1 : Description du Projet
- Annexe 2 : Répartition du budget et des moyens mobilisés par les établissements partenaires
- Annexe 3 : Volet général du projet
- Annexe 4 : Membres du Comité de Pilotage
- Annexe 5 : Liste des connaissances propres
- Annexe 6 : Organisation des relations entre l'académie de Martinique et le GIP-FCIP de l'académie de Martinique

SIGNATURES :

Pour le GRETA-CFA de la Guadeloupe

Nom : Elisabeth LEPIERRE

Fonction : CESUP

Signature : P/O Valérie GERAN
Directrice opérationnelle

Pour le Rectorat de la Guadeloupe

Nom : Gabriele FIONI

Fonction : Recteur

Signature :

Pour l'Agence Caribéenne pour la cybersécurité

Nom : Steven COCKS

Fonction : Président

Signature : 

Pour Orange Antilles-Guyane

Nom : Chantal MAURICE

Fonction : Directrice

Signature :

Pour le Rectorat de la Martinique

Nom : Nathalie MONS

Fonction : Rectrice

Signature :

Pour le GIP-FCIP de la Martinique

Nom : Olivier CHEVILLARD

Fonction : Directeur

Signature :

Pour l'Université des Antilles

Nom : Pr. Michel GEOFFROY

Fonction : Président

Signature :

APPEL A MANIFESTATION D'INTERET COMPETENCES ET METIERS D'AVENIR - CMA 2023

CATEGORIE : DISPOSITIF DE FORMATION

DOCUMENT PRESENTATION PROJET

CyberEDAntilles

Acronyme	CyberEDAntilles	
Titre du projet	Enseignement et développement de la cybersécurité aux Antilles	
Chef de file	**Raison sociale, structure juridique et N° Siret**	
	Université des Antilles, EPSCP, SIRET 19971585500011, Département 971 (Guadeloupe)	
Responsable du projet	**Nom, prénom et fonction**	
	Pr Erick Stattner Professeur des Universités en Informatique, Université des Antilles, Directeur Département Mathématiques-Informatique (DMI)	
	Courriel	**Téléphone**
	erick.stattner@univ-antilles.fr	Bureau: +(590) 590 48 34 31 Gsm. : +(596) 696 95 32 00
Durée du projet (max 60 mois)	**60 Mois**	
Aide totale demandée	**2 940 276 €**	
Coût total du projet	**5 079 322 € (hors frais d'environnement)** **5 522 257 € (avec frais d'environnement)**	
Merci de cocher le(s) volet(s) de l'AMI CMA concerné(s) par votre projet	☑ Les dispositifs transversaux d'attractivité et d'innovation ☑ Les voies d'excellence professionnelles et technologiques ☑ Les voies d'excellence académiques : ☑ Formation postbac, ☑Formation master, doctorat, attractivité internationale ☑ L'accompagnement des parcours professionnels	
Merci de cocher les secteur(s) éligible(s) aux priorités France 2030 (voir annexe 3 du cahier de charges de l'AMI - CMA)	**Faire émerger des réacteurs nucléaires de petite taille, innovants et avec une meilleure gestion des déchets** ☐ Nucléaire	

	Devenir le leader de l'hydrogène vert et des énergies renouvelables ☐ Devenir le leader de l'hydrogène vert **Décarboner notre industrie** ☐ Décarbonation de l'industrie ☐ Electronique et robotique ☐ Recyclabilité, recyclage et réincorporation de matériaux recyclés ☐ Technologies avancées pour les systèmes énergétiques ☐ Produits biosourcés et biotechnologies industrielles, carburants durables ☐ Solutions pour la ville durable et bâtiment innovant **Produire en France, à l'horizon 2030, près de 2 millions de véhicules zéro émission chaque année et développer une mobilité sobre, souveraine et résiliente** ☐ Véhicules connectés zéro émission ☐ Digitalisation et décarbonation des mobilités ☐ Batteries **Produire le premier avion bas carbone** ☐ Avion bas carbone **Investir dans une alimentation saine, durable et traçable afin d'accélérer la révolution agricole et alimentaire** ☐ Alimentation saine, durable et traçable ☐ Systèmes agricoles durables et équipements agricoles contribuant à la transition écologique **Produire 20 biomédicaments contre les cancers, les maladies chroniques dont celles liées à l'âge et créer les dispositifs médicaux de demain** ☐ Produire 20 biomédicaments ☐ Santé numérique ☐ Maladies infectieuses (ré)émergentes et menaces NRBC **Placer la France à nouveau en tête de la production des contenus culturels et créatifs** ☐ Industries créatives et culturelles **Prendre toute notre part à la nouvelle aventure spatiale**

	☐ Aventure spatiale **Investir dans le champ des fonds marins** ☐ Fonds marins **Souveraineté numérique** ☐ 5G et futures technologies de réseaux de télécommunications ☐ Cloud ☐ Intelligence artificielle ☐ Technologies du quantique **☑ Cybersécurité** ☐ Verdissement du numérique **Dispositifs transversaux d'innovation et d'attractivité** ☐ Enseignement et numérique ☐ Attractivité
Zone géographique de couverture du dispositif de formation (Veuillez préciser la/les région(s) visées)	• Guadeloupe • Martinique • Saint-Barthélemy • Saint-Martin
Type(s) de formation envisagé(s)	**☐ Scolaire ☑ Supérieur** **☑ Formation continue ☑ Sensibilisation**
Formation(s) / Titre(s) / Certification(s) visé(s)	• Licence informatique parcours Cybersécurité • Master MIAGE parcours Sécurité du numérique • Diplôme universitaire Cybersécurité • Titre de Technicien Supérieur Système Réseaux - option cybersécurité • Certification ISO 27001 • Certificat national CléA numérique • Accompagnement de dirigeants et chefs d'entreprise • Actions d'attraction vers la filière et de sensibilisation • Formation de formateurs en cybersécurité
Indiquer les sites sur lesquels les formations CMA seront publiées pour informer le public d'apprenants ciblés.	• Site internet de l'Université des Antilles • Site internet du GRETA-CFA de la Guadeloupe • Site internet du CARIF-OREF de la Guadeloupe • Plateforme nationale Mon Master • Salon virtuel de l'orientation en Guadeloupe
Branche(s) professionnelle(s) concernée(s) (si pertinent)	Personnel des prestataires de services du secteur tertiaire
Suite d'un projet CMA « Diagnostic »	**☑ Non ☐ Oui, préciser :**

Projets précédemment financés par le PIA ou France 2030	**☑ NON ☐ OUI, préciser :** **☐ *CMQe* ☐ *EUR* ☐ *IDEFI* ☐ *NCU*** **☐ *IFPAI* ☐ *PFPE*** **☐ *Autre* : ……**
Mots-clefs (1)	1. Cybersécurité 2. Antilles 3. Attraction et sensibilisation 4. Formations universitaires 5. Formation de formateurs 6. Alternance 7. Professionnalisation 8. Écosystème public-privé 9. Continuum pré-bac/post-bac 10. Hygiène numérique

(1) *Les expressions suivantes, trop génériques, ne sont pas permises :* FI, FC, FTLV, formation initiale, formation continue, formation tout au long de la vie, formation, compétences, métiers, innovation, transformation, pédagogie, outils pédagogiques innovants, enseignement scolaire, enseignement supérieur, entreprises.

LISTE DES MEMBRES DU CONSORTIUM (SI CONSORTIUM) – FOURNIR RAISON SOCIALE, STRUCTURE JURIDIQUE, N° SIRET ET N° DEPARTEMENT DE L'ÉTABLISSEMENT (cf. cahier des charges)

Organismes de formation ou d'accompagnement (universités, écoles, lycées, CFA, CFPPA, organismes privés, Pôle emploi/France Travail, associations, etc.).	***Secteur(s) d'activité***
Chef de file : Université des Antilles - EPSCP	Université, SIRET 19971585500011, Département 971 (Guadeloupe)
GRETA-CFA de la Guadeloupe	Groupement d'établissements publics locaux d'enseignement de l'Éducation Nationale, SIRET 19971405600025, Département 971 (Guadeloupe)
Agence caribéenne pour la cybersécurité	Association loi 1901, SIRET 91871489000012, Département 971 (Guadeloupe)

Donneurs d'ordre publics dans l'achat de formation (conseils régionaux, Pôle emploi/France Travail, OPCO,etc.)	***Secteur(s) d'activité***
Rectorat de la Région académique de Guadeloupe,	Rectorat, SIRET 17971430800238, Département 971 (Guadeloupe)
Rectorat de la Région académique de Martinique,	Rectorat, SIRET 1797243000030, Département 972 (Martinique)

Employeurs ou leurs représentants (entreprises, groupements d'employeurs, comité stratégique de filière, organisations professionnelles, syndicats, fédérations professionnelles , etc.)	***Secteur(s) d'activité***
Orange Antilles Guyane, Société anonyme	Entreprise secteur Télécoms, SIRET 38012986600519, Département 971 (Guadeloupe)

Recueil d'indicateurs à compléter de manière obligatoire sur le site de soumission CMA :

*Sur le site de soumission, vous devrez compléter de manière obligatoire l'onglet « **Informations Formations** ». Il s'agit d'un recueil d'indicateurs sur les formations envisagées dans le cadre votre projet, sur toute la durée du projet.*

Résumé du projet (Non confidentiel – 4000 caractères maximum, espaces inclus)

CyberEDAntilles est un dispositif ambitieux de formation initiale et continue en cybersécurité à destination du territoire antillais (Guadeloupe, Martinique, Saint-Barthélemy, Saint-Martin). Porté par l'Université des Antilles en collaboration avec un ensemble d'acteurs publics et privés, il a été élaboré sur la base d'un diagnostic révélant :

- des **lacunes dans l'offre de formation initiale et continue en cybersécurité**, générant un **déficit de compétences locales** ;
- une **forte vulnérabilité** aux cyberattaques, aussi bien pour les organisations publiques (collectivités) que pour les PME et TPE ;
- un **déficit de compétences et d'experts sur le territoire** pour répondre aux cybermenaces et participer aux actions de formations ;
- un **manque d'attractivité de la filière**, qui comporte pourtant un fort potentiel d'insertion professionnelle sur des territoires très touchés par le chômage ;
- l'importance d'une démarche de **formation de formateurs en cybersécurité** pour renforcer la souveraineté numérique du territoire.

Pour y répondre, CyberEDAntilles propose un **bouquet complet de formations** sur un continuum **du pré-bac à la formation supérieure et continue** pour développer des compétences expertes en matière de cybersécurité, ainsi que des **actions de sensibilisation** visant à renforcer le niveau de sécurité global du territoire. Il est articulé en **5 works-packages** :

1. **Sensibilisation et attraction vers la filière** : sensibilisation, acculturation et formation aux compétences de base vers les publics scolaires, les étudiants de l'Université et le grand public
2. **Formation initiale** : création d'un parcours « Cybersécurité » au sein de la Licence Informatique et d'un parcours « Sécurité du numérique » au sein du Master MIAGE
3. **Formation continue** : création d'un Diplôme universitaire Cybersécurité, préparation du Titre de Technicien Supérieur Système Réseaux - option cybersécurité, accompagnement des dirigeants et chefs d'entreprise
4. **Formation de formateurs et soutien à l'insertion professionnelle**
5. **Pilotage et communication**

Ces actions seront déployées par un **consortium multi-acteurs** réunissant l'**Université des Antilles**, les **Rectorats de Guadeloupe et de Martinique** (actions vers les publics scolaires) ; le **GRETA-CFA de Guadeloupe** (formation continue), l'**Agence caribéenne pour la cybersécurité**, (sensibilisation et la communication) ; **Orange Antilles-Guyane** (programme Orange Digital Center pour conduire une démarche de sensibilisation notamment vers les publics fragiles).

Le projet est également soutenu par un **réseau d'organisations souhaitant appuyer son déploiement**, par exemple en accueillant des apprentis ou en participant à la veille sur les besoins en compétences : Association du Numérique du Secteur Public, Chambre Économique Multiprofessionnelle de Saint-Barthélemy, CLUSIR, EXODATA, France Travail, Gendarmerie

nationale, Réseau CANOPE, OPCO AFDAS, UDE-MEDEF, collectivités territoriales (actions également envisagées avec le CNFPT et l'OPCO AKTO).

CyberEDAntilles mobilisera des **pédagogies innovantes** particulièrement adaptées à un contexte multi-insulaire, telles que des modalités hybrides et un recours à la réalité virtuelle. Les formations initiales et continues seront proposées en **alternance**, d'une façon qui favorisera l'insertion professionnelle et les interactions public-privé autour de la cybersécurité aux Antilles.

CyberEDAntilles sera déployé sur **5 ans**. Le coût complet du projet est de 5 079 322 €, dont 2 940 276 € de demande France 2030, et 2 139 046 € d'apport des partenaires. Il sera piloté par un **Comité de pilotage** assisté d'une **équipe opérationnelle** et d'un **Conseil pédagogique et stratégique**.

En répondant à un besoin avéré de création de compétences locales, CyberEDAntilles exercera un **impact mesurable sur la compétitivité de l'économie territoriale**, tout en renforçant la souveraineté numérique dans un Bassin marqué par une forte concurrence internationale.

Sommaire

1. DESCRIPTION DU PROJET DE DISPOSITIF(S) DE FORMATION ET D'ATTRACTIVITE

1. 1. PRESENTATION DU CONTEXTE

Dans une tribune récente[1], Bruno Bonnell, secrétaire général pour l'investissement en charge de France 2030, souligne l'**urgence du besoin de formations en cybersécurité**, dans un contexte marqué par une augmentation de plus de 37 % du nombre de cyberattaques entre 2020 et 2021 selon l'Agence nationale de la sécurité informatique (ANSSI). Comme le souligne cette tribune, cela exige « de décloisonner les filières dans l'informatique et de chasser l'*a-priori* voulant que la cybersécurité soit réservée aux techniciens et ingénieurs ».

CyberEDAntilles - Enseignement et développement de la cybersécurité aux Antilles répond directement à ce **besoin de formations plurielles en cybersécurité** aux Antilles françaises. Il a été élaboré sur la base d'un **diagnostic approfondi** concernant les **formations existantes** en Martinique et de Guadeloupe, les **compétences demandées sur le marché de l'emploi** et l'**incidence des cyberattaques** sur le territoire antillais. Ce diagnostic a été élaboré conjointement par l'Université des Antilles (UA), le Rectorat de la Guadeloupe, les DEETS Guadeloupe et Martinique, l'Agence caribéenne pour la cybersécurité et la Gendarmerie nationale.

Rôle des établissements d'enseignement supérieur dans la stratégie française cybersécurité : extrait de l'éditorial par Vincent Strubel, Directeur général de l'ANSSI, Sécurité des SI : La cybersécurité au cœur de la stratégie de l'ESRI (fév. 2024)

> A la veille de la transposition de la directive NIS 2 en droit français qui oblige les Etats membres à adopter une stratégie nationale concernant l'éducation et la formation, la recherche et le développement en matière de cybersécurité[1], nous encourageons les ESRI à se mobiliser afin qu'ils développent une plus grande **culture de la gestion du risque cyber et s'approprient les objectifs de cybersécurité** à atteindre. La France a besoin de s'appuyer sur des générations diplômées et acculturées au risque cyber.

En particulier, l'UA et le Rectorat de Guadeloupe sont parties prenantes des **travaux relatifs à l'EDEC numérique lancés par la DEETS Guadeloupe**[2], qui aboutiront à la mise en place d'un plan de formation coordonné. Les fiches prospectives proposées pour les différentes branches professionnelles révèlent en effet que la Guadeloupe est perçue comme un **territoire vulnérable aux risques cyber**, avec un niveau de compétences variable selon les acteurs, et un besoin réel d'accompagnement, notamment pour les **TPE/PME** dont est principalement composé le tissu économique du territoire. Dans de nombreux secteurs, il est essentiel de mettre en place un **socle de compétences techniques et transverses en matière de cybersécurité et de sécurisation des données**, ainsi qu'une **formation de professionnels de la cybersécurité** (techniciens cybersécurité, Data Protection Officers, consultants cybersécurité, analystes/techniciens Security Operations Center...). Par ailleurs, le diagnostic souligne un **manque d'attractivité** pour les métiers de la cybersécurité en Guadeloupe, en raison d'un décalage entre l'image et la réalité du métier, d'un manque de passerelles avec d'autres métiers et d'une offre de formation jugée inadéquate par les professionnels. C'est pourquoi il recommande d'« **intégrer les compétences techniques et transverses de cybersécurité dans les cursus des formations initiales en Numérique**, développer une **offre certifiante** et des **passerelles** sur les métiers spécifiques à la cybersécurité, accessible à niveau Bac+2 ou Bac+3 (...), créer des **passerelles entre les métiers de la cybersécurité et les métiers du réseau** (administrateurs systèmes et réseaux) ».

En **Martinique**, le Contrat d'Étude Prospective Métiers du Numérique (conclusions préliminaires - janvier 2024) démontre également d'importantes opportunités de développement économique dans

[1] Tout le monde peut travailler dans la cybersécurité !, La Tribune, novembre 2023.
[2] Source : EDEC Numérique Guadeloupe DEETS-AKTO/ATLAS.

le secteur de la cybersécurité, mais aussi une structuration insuffisante de la formation.

Cybersécurité en Martinique : Opportunités	Cybersécurité en Martinique : Faiblesses
Nouvelles **opportunités de marché** Levier pour le développement du **commerce en ligne** Stratégie de mise en place d'un **territoire souverain numériquement** Devant le risque accru de cyberattaque, les **commissaires aux comptes** vont demander de faire des provisions pour le risque cyber Les **assurances** vont mettre en place des questionnaires très précis sur les actions cybersécurité menées par les entreprises et en fonction de la criticité de leurs activités, décideront de les assurer ou non.	**Lacunes de l'offre de formation : Difficultés de recrutement niveau ingénieur/Bac+5**, problèmes d'adaptation des ingénieurs de l'Hexagone, les **titulaires d'un BTS ou DUT** qui souhaitent poursuivre en étude d'ingénieurs doivent partir se former en dehors, une **offre de formation continue** qui fait défaut, au sein de l'**Université des Antilles** : Licence informatique générale, mais pas de module cybersécurité **Difficulté à trouver de bons formateurs** **Manque de compétences au sein du tissu entrepreneurial et manque d'anticipation** : les chefs d'entreprise doivent être formés aux risques de cyberattaques et incités à la **réalisation d'audit et l'analyse des risques** **Concurrence internationale** au sein du Bassin
Recommandations	
Création de formations spécifiques à la cybersécurité : auditeur, chef de projet cybersécurité, architecte cybersécurité, formations certifiantes (ANSSI), modules cybersécurité au sein de formations transverses... **Actions de sensibilisation et d'acculturation** sur la digitalisation et la cybersécurité Mise en place de **formations continues sur la cybersécurité** Continuer à développer l'**alternance** Rendre la **formation professionnelle** plus lisible, plus accessible **Mise en avant de certains métiers** : RSSI, chef de projet Cyber, Architecte Cloud-Cyber… **Plus forte intégration dans les formations des enjeux cybersécurité** et de transition environnementale Mettre en place une **formation de formateurs**.	

Si des formations courtes pré ou post-bac en cybersécurité ainsi qu'une offre de formation privée existent en Guadeloupe et en Martinique[3], il y a aujourd'hui un manque de **formations expertes de niveau licence ou Master**, ainsi qu'au niveau de la **formation continue**. L'offre est par ailleurs dispersée et peu lisible, et il n'existe pas à ce jour de **dispositif intégré** proposant un **bouquet complet de formations** avec une identité thématique sur l'ensemble du continuum depuis le pré-bac jusqu'au post-bac et à la formation continue. Il existe pourtant un **potentiel à la fois en termes de vivier étudiant et de personnel enseignant**, puisque l'UA propose notamment une licence en informatique, ainsi qu'un Master Informatique et un Master Méthodes Informatiques Appliquées à la Gestion des Entreprises (MIAGE). Cependant, comme le souligne le diagnostic cité plus haut,

[3] Guadeloupe : Bac Pro CIEL, Mention complémentaire Cybersécurité ; BTS cybersécurité, informatique et réseaux, électronique option A informatique et réseaux ; Plateforme privée de formation numérique Concept X Formation, Certifications proposées par des opérateurs privés (M2i, Webforce3), Modules proposés par le CNAM Guadeloupe et par la CCI Guadeloupe. Martinique : Bac Pro CIEL, Mention complémentaire Cybersécurité ; BTS cybersécurité, informatique et réseaux, électronique option A informatique et réseaux ; BTS Services Informatiques aux Organisations, option SISR en alternance (CCI Martinique et CFA Skillfor) ; Métiers des Réseaux Informatiques et Télécommunications parcours Administration et Sécurité des Systèmes - 3ème année (CCI Martinique et CFA Skillfor) ; L3 STS mention Informatique Générale option Cybersécurité (CNAM Martinique) ; Modules de formation continue proposés par le CNAM Martinique ; Modules de formation continue proposés par des organismes privés (M2i, Unichrone).

l'Université ne propose pas de formations spécifiques en cybersécurité[4], et les jeunes souhaitant se spécialiser doivent donc soit se tourner vers des opérateurs de formation privés, soit aller étudier dans l'Hexagone, ce qui génère des inégalités territoriales.

Le développement d'une telle offre de formation est d'autant plus fondamental que **le territoire antillais a fait l'objet de nombreuses cyberattaques** au cours des dernières années : LADOM en 2015, plusieurs dizaines de TPE/PME en Guadeloupe en 2020, Collectivité Territoriale de Martinique en 2022-2023, Conseil régional de la Guadeloupe en novembre 2022, puis nouvelle cyberattaque par des hackers pro-russes en février 2024. La capacité à lutter efficacement contre ces menaces requiert le développement de **compétences internalisées** et une formation à l'identification des menaces au sein du Bassin caribéen et de son environnement international.

En France, le secteur de la cybersécurité est par ailleurs un **secteur en tension**, avec **15 000 postes non pourvus**, et environ **37 000 postes qui devraient être créés à horizon 2030**[5]. La Stratégie nationale d'accélération sur la cybersécurité se donne quant à elle pour objectif de passer de 37 000 à 75 000 emplois en cybersécurité à Horizon 2025[6]. Ces besoins s'accroîtront avec différents facteurs comme le **passage à la facturation électronique obligatoire**, ou encore le **Cyber Resilience Act** et la **Directive NisV2** adoptée par l'Union européenne qui renforce les règles en matière de cybersécurité. Cela implique une **insertion professionnelle** importante, et des **conditions attractives** avec un salaire d'entrée souvent plus élevé que la moyenne. Cette opportunité est particulièrement valorisante dans le contexte antillais, puisque **27% des jeunes de 15 à 29 ans en Guadeloupe ne sont ni en emploi, ni en études, ni en formation**[7], et que ce pourcentage est de **26% en Martinique**[8], soit deux fois plus que dans l'Hexagone.

Profil type d'un professionnel de la cybersécurité

- Un homme
- De 30 à 49 ans
- De niveau de qualification Bac +5
- Issu du domaine informatique/numérique
- De moins de 10 ans d'expérience dans la cybersécurité
- Travaillant en Ile-de-France
- Salarié du secteur privé
- Travaillant au sein d'une équipe de professionnels de la cybersécurité
- Travaillant dans une structure de 1 000 salariés et plus
- Travaillant dans une structure non spécialisée en cybersécurité
- Consultant cybersécurité ou RSSI
- 100% de son temps est consacré aux questions de cybersécurité
- Plutôt recruté via le marché caché
- Régulièrement sollicité par des recruteurs

Afin de faciliter la création d'emplois et de diversifier les profils, il est fondamental de travailler sur l'**attractivité de cette filière**. L'enquête réalisée par l'ANSSI en 2021 sur les Profils de la cybersécurité révèle en effet un profil souvent monolithique en cybersécurité, qu'il serait intéressant d'ouvrir davantage vers un public féminin, plus jeune, ouvert aux formations courtes et aux compétences transversales, éloigné des grands centres métropolitains, susceptible d'être employé par le secteur public et/ou dans un environnement économique composé en grande partie de TPE et de PME.

○ 1. 2. DESCRIPTION DU OU DES DISPOSITIFS DE FORMATION ET/OU D'ATTRACTIVITE

■ 1. 2. 1. Les métiers et compétences

De par son large spectre d'intervention, CyberEDAntilles permettra aussi bien de former des **publics de formation initiale et continue** sur des métiers spécifiques au domaine de la cybersécurité que de garantir un **socle de compétences** en cybersécurité au sein de **métiers aux interfaces**. Les

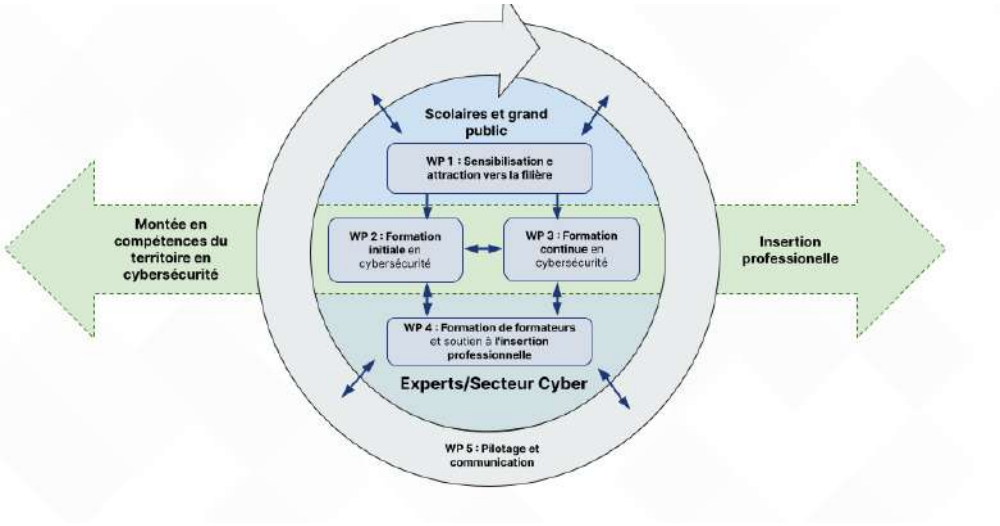
[4] Un projet de formation avait été accrédité en 2018 mais n'avait pas abouti faute d'enseignants spécialistes.
[5] Cybersécurité : où en sont les grandes entreprises françaises, Wavestone, 2022.
[6] Source : Communiqué de presse du Gouvernement.
[7] Source : INSEE.
[8] Source : INSEE.

métiers directement liés aux compétences clés de la cybersécurité seront notamment : Administrateur système/réseau/base de donnée ; Administrateur d'infrastructures sécurisées ; Responsable de la sécurité des systèmes d'information ; Consultant en sécurité informatique ; Architecte systèmes et logiciels ; Ingénieur en Cybersécurité ; Technicien Supérieur Système Réseaux ; Responsable de la sécurité des systèmes d'information ; Consultant en sécurité informatique.

L'acquisition de **socles de compétences** en cybersécurité permettra également aux professionnels formés d'aborder les problématiques de sécurité du numérique dans des domaines variés, par exemple Banque - finance - assurance, Administration, Économie - comptabilité - gestion - finances, Industrie - qualité - gestion des risques, Informatique - télécommunication, Marketing - commerce - distribution, Médias - communication - audiovisuel, Numérique - multimédia - web, Ressources humaines - management, Santé, Social ou encore Transport.

En formant non seulement des futurs professionnels de la cybersécurité, mais en développant des compétences transversales utiles dans tout un ensemble d'autres secteurs, CyberEDAntilles répond aux enjeux du développement des compétences numériques, qui sont ceux d'une transformation de l'ensemble de l'économie à travers ce levier.

■ 1. 2. 2. Le projet



Périmètre et consortium : CyberEDAntilles propose un bouquet de formations à destination d'un continuum allant du **public pré-bac** (sensibilisation et attraction vers la filière) au **public post-bac de la formation initiale**, **l'alternance et la formation continue**. Elles s'adresseront en premier lieu au **public du territoire antillais** (Guadeloupe, Martinique, St-Barthélémy, St-Martin), mais seront également ouvertes à un **public plus large au sein du Bassin caribéen** (p. ex. : Sint Maarten). Les enjeux de souveraineté nationale sont particulièrement marqués au sein du Bassin compte tenu de la présence proche de l'industrie nord-américaine, renforçant l'importance d'une structuration à l'échelle du Bassin au service du rayonnement de la France dans la région.

CyberEDAntilles est proposé par un **consortium** ambitieux réunissant des acteurs publics de la formation initiale et continue, ainsi que des acteurs privés territoriaux. Il est porté par l'**Université des Antilles**, établissement-phare de l'enseignement supérieur aux Antilles, et comprend des représentants des employeurs (**Orange Antilles-Guyane**), des organismes de formation et d'accompagnement (**GRETA-CFA de Guadeloupe, Agence caribéenne de cybersécurité**) et des donneurs d'ordre publics dans l'achat de formation continue des chercheurs d'emploi (**Rectorats de Guadeloupe et de Martinique**). CyberEDAntilles a de plus constitué un **réseau d'organisations publiques et privées** exprimant l'intention d'en faciliter le déploiement, par exemple en accueillant des apprentis ou en contribuant à la veille sur les besoins en compétences : Association du Numérique du Secteur Public, Chambre Économique Multiprofessionnelle de Saint-Barthélemy,

CLUSIR, EXODATA, France Travail, Gendarmerie nationale, Réseau CANOPE, OPCO AFDAS (actions également envisagées avec l'OPCO AKTO et le CNFPT), UDE-MEDEF. La Collectivité territoriale de Martinique est associée au projet. La Région Guadeloupe le sera également, notamment via l'Agence Caribéenne pour la Cybersécurité et le Rectorat de Guadeloupe.

Structuration du projet

CyberEDAntilles est pleinement aligné avec la **Stratégie Nationale Cyber**, et notamment avec son **Axe 4 - Former plus de jeunes et professionnels aux métiers de la cybersécurité**. Il a été conçu en adéquation étroite avec les attendus de la fiche thématique Cybersécurité, qui formule deux priorités :

- **Former davantage de personnes aux métiers de la cybersécurité incluant toutes les déclinaisons de niveau de spécialisation** en fonction des postes visés pour répondre à la très forte demande en compétences du secteur et soutenir sa croissance
- **Former le plus grand nombre aux enjeux, dangers et gestes simples de la cybersécurité** à la fois pour soutenir la demande mais aussi, et surtout, pour élever le niveau de sécurité global du pays

Pour relever ces deux défis, CyberEDAntilles se déploie en **5 work-packages** présentés ci-après.

Work-package 1 : Sensibilisation et attraction vers la filière
Objectifs - Attraction des jeunes/des publics scolaires vers les formations en cybersécurité, avec un focus sur les publics éloignés (notamment public féminin) - Acculturation et initiation aux compétences de base en cybersécurité dans des secteurs transverses - Élévation du niveau de compétences en cybersécurité au service d'une transformation de l'économie
Description des actions **Sous-WP 1. 1. Attraction vers la filière au collège (3ème) et au lycée**, en partenariat avec les Rectorats de Guadeloupe et de Martinique. En Guadeloupe, l'Académie dispose de 9 Fab'Labs équipés et aménagés par les collectivités (Région Guadeloupe et Collectivité de Saint-Martin) dans 9 lycées répartis sur le territoire. La sensibilisation sera menée à travers 2 types d'ateliers dispensés en priorité au sein de ces Fab'Labs : ateliers de sensibilisation pour les élèves de 3ème et 2nde et ateliers avancés de sensibilisation pour les élèves de Terminale et de BTS. Les enseignants bénéficieront des ressources de CANOPE Guadeloupe[9] pour la sensibilisation à la cybersécurité et à l'hygiène numérique. L'ingénierie pédagogique sera élaborée par les enseignants en cybersécurité de l'Académie, accompagnés d'experts. Les modules seront ensuite déployés à travers l'animation des ateliers précités. Afin de permettre l'initiation et les mises en situation concrètes, le projet mettra à disposition des équipements informatiques dédiés au sein de 3 Fab'Labs dans un premier temps, puis des 6 autres avec l'appui de la Région Guadeloupe. Une articulation sera prévue avec des événements tels que Demain spécialiste cyber, la Semaine du numérique et des sciences informatiques, Capture the flag : Passe ton Hack d'abord de la 2nde à Bac+2[10] co-organisé par le commandement de la cyberdéfense et la Direction générale de l'enseignement scolaire. En Martinique, on valorisera les actions du Safer Internet Day et la Semaine du numérique en ciblant la

[9] Voir par exemple cette vidéo.

[10] Secondes GT SNT, professionnelle Métiers des transitions numérique et énergétique ; premières/terminales G spécialité mathématiques et NSI, technologiques filières STMG et STI2D, professionnelles filière CIEL ; BTS CIEL, SIO et mentions complémentaires SNO et cybersécurité.

cybersécurité pour les écoles, collèges et lycées. Le projet conduira à concevoir un escape game pour les élèves de 3ème (1 séance de 2h pendant 3 ans), ainsi qu'un défi Capture the flag : Passe ton Hack d'abord pour les élèves de 2nde.

Sous-WP 1. 2. Sensibilisation à la cybersécurité et promotion de l'hygiène numérique à destination du grand public à travers les actions suivantes :

- Création d'une version améliorée du « Serious Game » Opération Skybreak (mis en place par l'ACCYB) qui aura la capacité d'atteindre un public plus large
- Mise en place d'un Hackathon Formation en présentiel en s'appuyant sur le Hackathon Challenge, en lien avec la cybersécurité, organisée par l'ACCYB
- Montée en puissance du programme Orange Digital Center avec des ateliers numériques d'acculturation autour de 6 thématiques : Sécurité et confiance numérique, Protection des données personnelles, Se protéger des arnaques en ligne, Protection de son identité numérique, Réseaux sociaux et esprit critique, Jeunes et cyber harcèlement. Publics visés : jeunes adultes fragiles, accessibles par les missions locales et le RSMA ; jeunes en formation d'adulte, accessibles via les CFA académiques ; publics séniors, accessibles par les associations de séniors, les CCAS et autres structures communales. Une formation d'animateurs sera mise en place pour étoffer les ressources humaines et faciliter le déploiement des ateliers, parmi les apprenants en formation d'animation sociale et socio-culturelle et de la relation client.
- Soutien au renforcement de l'utilisation du CléA numérique, une certification interprofessionnelle reconnue nationalement garantissant l'acquisition d'un socle de connaissances et de compétences commun (voir module 4, Appliquer les règles et bonnes pratiques de la sécurité numérique)

Sous-WP 1. 3. Modules d'initiation aux compétences de base en cybersécurité les publics post-bac et les étudiants de l'UA (L1 et L2) ouverts aux primo-entrants de l'UA, aux stagiaires de la formation continue et aux salariés des administrations et entreprises qui pourront donner lieu par la suite à une offre de micro-certification. Tous les primos-arrivants de l'UA seront sensibilisés via un appui sur le référentiel PIX (Sécurisation de l'environnement des pratiques numériques). Un module d'enseignement spécifique sera introduit en L2 pour les mathématiciens et informaticiens.

Nombre d'heures prévisionnelles

- Actions de sensibilisation/attraction pour les scolaires : séances de 1 à 2h selon les formats
- Modules d'initiation aux compétences de base : L1 : 10h, L2 MATHS-INFO : 24h
- Modules de formation aux compétences numériques de base et à l'hygiène numérique : 74h

Titres, certifications ou diplômes proposés : Certificat national CléA numérique ; à terme, micro-certifications cybersécurité pour les professionnels et stagiaires de la formation continue

Débouchés : Orientation des jeunes vers les formations en cybersécurité

Partenaires impliqués

- Rectorats de Guadeloupe et de Martinique (pilotes)
- ACCYB (événementiel de sensibilisation) (pilote)
- Université des Antilles (modules de sensibilisation pour les étudiants de L1/ L2)
- Orange Antilles-Guyane (mobilisation du programme Orange Digital Center)
- GRETA-CFA de la Guadeloupe (déploiement du CléA numérique)
- Organisations soutenant le projet, dont AFDAS (mobilisation et financement autour du CléA numérique)

Estimation du public touché

- Sensibilisation en collège et lycée : 720 lycéens et collégiens/an
- Sensibilisation grand public : escape game : 400 personnes/an, hackathons : 100 personnes/an, Ateliers Orange Digital Center : 1 000 personnes/an en comptant les 4 territoires
- Modules d'initiation compétences de base : plusieurs centaines d'étudiants par an (primo-entrants, L2)
- CléA numérique : 30 salariés/an

Work-package 2 : Formation initiale en cybersécurité

Objectifs
- Proposer une offre complète de formation initiale en cybersécurité afin de garantir un vivier de professionnels formés à ces compétences sur le territoire
- Proposer une offre de formation experte et certifiante en cybersécurité
- Favoriser l'insertion professionnelle, notamment à travers un dispositif de formation en alternance

Description des actions
Sous-WP 2. 1. Création d'un parcours « Cybersécurité » au sein de la Licence Informatique, accessible en alternance - public ciblé : BTS CIEL, BUT INFO, Licence 2 Informatique ou équivalent. Ce parcours enrichira l'éventail de formations déjà disponibles à l'UA, où deux autres parcours de la licence, Informatique et MIAGE, conduisent respectivement vers des Masters en Informatique et en MIAGE. Ce nouveau parcours vise un double objectif: (i) acquérir le socle fondamental de connaissances et de compétences de la cybersécurité ; (ii) préparer à une poursuite en Master sur la sécurité des systèmes d'informations. L'introduction de ce parcours ne perturbera pas les effectifs des formations existantes, car il cible principalement les étudiants issus des BTS CIEL et du BUT INFO, déjà sensibilisés à la cybersécurité et sans perspectives de poursuite d'études locales. Enfin, ce parcours aura une dimension professionnalisante forte, puisqu'il sera ouvert exclusivement en alternance avec participation de professionnels du territoire.
Sous-WP 2. 2. Création d'un parcours « Sécurité du numérique » au sein du Master MIAGE de l'UA - Public ciblé : Licence 3 Informatique - parcours Cybersécurité ou équivalent. Le Master MIAGE vise à donner une double compétence aux étudiants : en Informatique et en Gestion des entreprises. Le parcours « Sécurité du numérique » s'ajoutera au parcours existant « Science des données et Application » et aura pour objectif de former des cadres avec un haut niveau d'expertise en cybersécurité. Il sera ouvert exclusivement en alternance et facilitera les contrats d'apprentissage et de professionnalisation dans les différents territoires du projets avec des périodes d'apprentissage longues (entre 2 et 3 mois). Il inclura également la préparation à la certification ISO 27001 durant l'année de Master 2.

Nombre d'heures prévisionnelles
- Parcours Cybersécurité Lic. Informatique : 500h (dont 40 % réalisées par des professionnels du territoire)
- Parcours « Sécurité du numérique » Master MIAGE : 500h en Master 1ère année (dont 40 % réalisées par des professionnels du territoire), 400h en Master 2ème année (dont 10 % dédiées à la préparation et de la certification et 40 % réalisées par des professionnels du territoire)

Titres, certifications ou diplômes proposés : Licence Informatique parcours Cybersécurité, Master MIAGE parcours Sécurité du numérique, Préparation à la Certification ISO 27001 en Master 2

Débouchés
- Poursuite en Master et/ou en Doctorat

- Insertion professionnelle : Administrateur système/réseau/base de donnée, Responsable de la sécurité des systèmes d'information, Consultant en sécurité informatique, Architecte systèmes et logiciels, Ingénieur en Cybersécurité, Délégué à la protection des données, Chef de projet informatique

Partenaires impliqués
- **Université des Antilles (pilote)**
- **GRETA-CFA de la Guadeloupe** (mise en œuvre formations en apprentissage et professionnalisation)
- Réseau des organisations soutenant le projet (Orange, EXODATA, Gendarmerie Nationale) : accueil et recrutement des alternants

Estimation du public touché
- Parcours cybersécurité au sein de la licence informatique : 10 à 15 étudiants/an
- Parcours Sécurité du numérique au sein du Master MIAGE : 8 à 12 étudiants/an

Work-package 3 : Formation continue en cybersécurité

Objectifs
- Faciliter la montée en compétences des professionnels en cybersécurité
- Favoriser les reconversions professionnelles dans le domaine de la cybersécurité
- Proposer une offre de formation aux demandeurs d'emploi
- Mettre en place un modèle vertueux en cascade : former des profils clés au sein des organisations qui poursuivront la formation des salariés en interne

Description des actions

Sous-WP 3. 1. Accompagnement des **dirigeants et chefs d'entreprises** pour leur proposer un diagnostic action au niveau RH et organisationnel dans le domaine de la cybersécurité

Sous-WP 3. 2. Création d'un Diplôme universitaire Cybersécurité adressé à des salariés ou demandeurs d'emploi titulaires d'un BTS ou DUT en informatique (bac+2) et plus, accessible en alternance ou en formation continue pour former des professionnels capables de maîtriser, analyser, concevoir, implémenter des solutions de sécurité des systèmes et réseaux informatiques. Inclut une préparation à la certification ISO 27001.

Sous-WP 3. 3. Préparation du Titre de Technicien Supérieur Système Réseaux - option cybersécurité accessible en alternance : formation de professionnels qui maîtrisent l'installation, le maintien du fonctionnement et de l'utilisation d'infrastructures informatiques, et accompagnent les utilisateurs tant dans la prise en main qu'au niveau des dysfonctionnements. Ils interviennent également sur la sécurité des réseaux, du diagnostic à la résolution de dysfonctionnements. La polyvalence de ce professionnel en fait un véritable atout pour les petites entreprises. Cette formation pourra être complétée par le DU cybersécurité (compétences expertes).

Titres, certifications ou diplômes proposés : Diplôme universitaire Cybersécurité, Titre professionnel de Technicien Supérieur Système Réseaux - option cybersécurité, de niveau 5, préparation à la Certification ISO 27001

Nombre d'heures prévisionnelles
- Diplôme universitaire Cybersécurité : 180h
- Préparation du Titre de Technicien Supérieur Système Réseaux - option cybersécurité : 900h

Débouchés : Administrateur système/réseau/base de données, Administrateur d'infrastructures sécurisées, Technicien Supérieur Système Réseaux, Responsable de la sécurité des systèmes d'information, Consultant en sécurité informatique

Partenaires impliqués
- GRETA-CFA de Guadeloupe (pilote)
- Université des Antilles (mise en place du Diplôme Universitaire)
- ACCYB (accompagnement des entreprises)
- Organisations soutenant le projet (OPCO AFDAS, Orange Antilles-Guyane, CLUSIR, EXODATA, Gendarmerie Nationale, UDE-MEDEF, France Travail (actions également envisagées avec l'OPCO AKTO et le CNFPT) : accueil d'alternants, promotion des actions

Estimation du public touché
- Diplôme universitaire : 15 apprenants par an à partir de la rentrée 2025/2026
- Titre de Technicien Supérieur Système Réseaux - option cybersécurité : 15 apprenants /an
- Accompagnement des dirigeants : 55/an
- Certifications Iso 27001 : 30 apprenants/an

Work-package 4 : Formation de formateurs et soutien à l'insertion professionnelle

Objectifs
- Formation de formateurs garantissant la pérennité du dispositif
- Soutien à l'insertion professionnelle et rétention des talents et des compétences sur le territoire

Description des actions
Sous-WP 4. 1. Formation de formateurs (enseignants-chercheurs de l'UA, personnels des Rectorats, formateurs du GRETA-CFA) à travers la mobilisation de formateurs professionnels, conduite sur les 2 premières années du projet. Inclut une capacité à former à la préparation de la certification ISO 27001
Sous-WP 4. 2. Soutien à l'insertion professionnelle en interaction avec France Travail et avec le réseau des entreprises partenaires, notamment via la mobilisation du Conseil pédagogique et stratégique (voir section 2. 2. 2. ci-dessous), composé d'experts du territoire et de représentants du tissu économique

Nombre d'heures prévisionnelles Formation de formateurs : 30h

Partenaires impliqués
- GRETA-CFA de Guadeloupe (pilote)
- Université des Antilles, Rectorats de Guadeloupe et de Martinique (vivier de personnels formés)
- ACCYB, France Travail, autres organisations soutenant le projet (interface avec les employeurs)

Estimation du public touché Formation de formateurs : 30 personnels au total

Work-package 5 : Pilotage et communication

Objectifs
- Mettre en place un dispositif de pilotage collégial et efficace du projet
- Assurer l'amélioration continue et l'adaptation des formations à l'évolution des compétences

- Garantir un suivi appuyé sur les données à travers un recueil d'indicateurs pertinents - Garantir la pérennité du projet - Assurer la communication autour des formations ainsi que leur promotion, mettre en place une communauté de pratiques et créer une dynamique autour du projet
Description des actions **Sous-WP 5. 1. Mise en place des instances de pilotage du projet et de l'équipe-projet** (voir sections 2. 1. et 2. 2. ci-dessous) **Sous-WP 5. 2. Mise en place d'un système de suivi** appuyé par un recueil d'indicateurs pertinents (voir section 2. 2. ci-dessous) **Sous-WP 5. 3. Élaboration et déploiement d'un plan de communication autour des formations** (supports de communication diffusés auprès des publics scolaires, communication sur les réseaux sociaux et dans les médias locaux, communication auprès des entreprises) **Sous-WP 5. 4.** Organisation et participation à des **événements de promotion des formations** (Salons, Semaine de l'alternance, Forum des métiers etc.) (voir détail en section 1. 4.) **Sous-WP 5. 5. Animation d'une communauté de pratiques** autour des formations
Partenaires impliqués **- Université des Antilles (pilotage) et ACCYB (communication et communauté de pratiques)** - Ensemble des partenaires du projet (gouvernance du projet et actions de communication) - Organisations soutenant le projet : communication et promotion des actions

■ 1. 2. 3. Les modalités pédagogiques et d'accompagnement

Les formations du dispositif CyberEDAntilles seront proposées **sur les territoires de Guadeloupe, Martinique**, et ouvertes au public de **Saint-Martin et Saint-Barthélemy**. Dans le cas des formations initiales de licence et de Master (WP2), les cours magistraux seront conduits en **modalité hybride**, et les TD seront dédoublés (conduits en présentiel sur chacun des deux pôles de l'UA). Dans ses différents domaines d'implémentation, CyberEDAntilles mobilisera des **formats pédagogiques innovants et attractifs** qui incluront une **formation par la pratique, réalisée notamment en articulation :**

- **avec les Rectorats de Guadeloupe et de Martinique** pour une sensibilisation au collège et au lycée appuyée sur des pratiques ludiques sur le modèle du dispositif Cyberenjeux proposé par l'ANSSI et à travers l'utilisation de fablabs dédiés ;
- en articulation avec le projet d'**Institut du numérique** en cours de consolidation par la **Collectivité territoriale de Martinique** et avec le projet de **Laboratoire cyber** de **l'ACCYB** mis en place en Guadeloupe, un lieu de type Fablab permettant de réaliser des tests en matière de sécurité (p. ex. : tests sur des virus nécessitant des espaces fermés/sécurisés).

De plus, CyberEDAntilles s'appuie sur le dispositif de la **formation en alternance,** qui permettra de renforcer le lien avec le monde socio-économique et l'insertion professionnelle des apprenants. CyberEDAntilles mobilisera également des techniques de **réalité virtuelle**, sur la base d'une première expérimentation pilote conduite par des enseignants-chercheurs de l'UA qui a démontré la valeur ajoutée de l'apprentissage par réalité virtuelle, notamment au sein des enseignements en informatique[11]. Nous procéderons à l'équipement de 2 **salles de TD pour enseignements**

[11] Pluton, L. et Stattner, E. (2023). Influence de l'envir ne nt de formation à distance sur l'engagement des apprenants et apprenantes : une expérimentation autour de la réalité virtuelle.

hybrides/technologies Hyflex sur les Pôle de Guadeloupe et de Martinique de l'Université.
CyberEDAntilles a pour particularité de préparer les futurs professionnels antillais aux **spécificités de ce secteur sur leur Bassin géographique**. En plus du socle de compétences fondamentales et techniques, il proposera des **modules complémentaires et pluridisciplinaires liés aux aspects juridiques, géopolitiques ou économiques propres au Bassin caribéen** : origine des attaques, gestion de crise en écosystème insulaire, spécificités juridiques locales, infrastructures.
Les formations mises en place seront labellisées à travers le LABEL SECNUMEDU (formations longues) et le LABEL SECNUMEDU formation continue. Des intervenants seront mobilisés à travers les **réseaux d'experts** des partenaires, notamment l'ACCYB. Lorsque des prestataires externes seront mobilisés, ceux-ci seront sélectionnés sur la base de critères de qualité (certification Qualiopi), et dans le respect des règles de la commande publique.

■ 1. 2. 4. Les mesures en faveur de la transition sociétale

CyberEDAntilles est pensé dans une démarche d'inclusivité, aussi bien du point de vue des publics visés que des intervenants au sein des formations. Cela se traduira notamment par :

- un **ciblage des publics éloignés** (public féminin, publics fragiles, dans les **actions de sensibilisation/attraction vers la filière** ;
- un **ciblage des publics vulnérables** (publics séniors, recours à la langue créole dans les formations) dans les actions de sensibilisation à l'hygiène numérique ;
- une cible d'**un tiers de femmes** minimum pour les actions de **formation de formateurs**, de façon à garantir ce même ratio au sein du vivier de formateurs du dispositif.

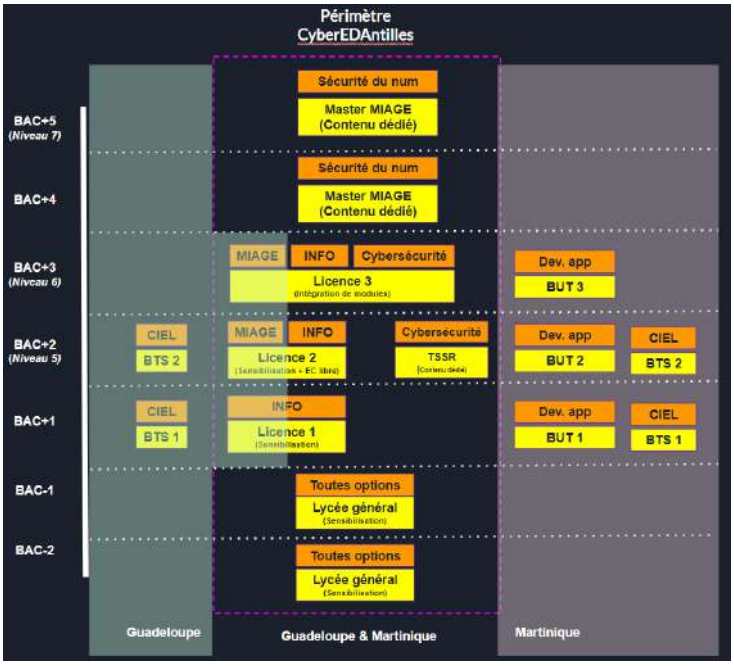
Cette politique d'inclusivité est notamment au centre de la stratégie du programme **Orange Digital Center**, partenaire du projet dont l'une des priorités est de s'adresser à des publics éloignés ou fragiles (Quartiers politiques de la ville, mobilisation d'experts de l'inclusion des séniors, prise en compte de l'illectronisme, accompagnement à l'entrepreneuriat féminin digital).
En termes de **transition environnementale**, un défi propre au projet tient à la multi-insularité de son champ de déploiement (Guadeloupe, Martinique, St-Martin, St-Barthélemy). Les mesures de **pédagogie hybride** mentionnées plus haut auront notamment pour fonction de **limiter l'impact environnemental** du projet en évitant les déplacements des formateurs ou des apprenants. Par ailleurs, le fait de procéder à des actions de **formation de formateurs**, puis de former un **vivier de compétences locales** en cybersécurité permettra d'internaliser ces compétences et d'éviter de mobiliser des experts en provenance de l'Hexagone.

○ 1. 3. RESULTATS ET MESURE DE L'IMPACT

Sur la base des effectifs moyens par action proposés dans la description des work-packages ci-dessus, nous estimons que le dispositif CyberEDAntilles permettra de former et sensibiliser directement **4 200 personnes**[12] au total au bout des 5 ans de la période de financement, en tenant compte de l'amorçage puis de la montée en puissance. Au-delà de cette période (en rythme de croisière une fois le dispositif parvenu à maturité), il est attendu que près de **950 personnes par an** soient directement formées et/ou sensibilisées. En plus de cela, des centaines de personnes sur les 4 territoires de déploiement du projet seront touchées par les actions de sensibilisation destinées au grand public (Escape game, hackathon, Orange Digital Center, événementiel etc.).
En termes de **risques**, le principal risque identifié tient à la capacité à **dégager un vivier suffisant de participants aux formations**, notamment sur un ensemble de territoires insulaires. Ce risque est néanmoins jugé comme contrôlé à travers une analyse des flux de publics-cibles au sein du

[12] Nous avons révisé l'estimation du public touché par le dispositif CyberEDAntilles par rapport à la lettre d'intention en faisant une distinction plus claire entre les personnes directement formées/sensibilisées et les actions de sensibilisation destinées au grand public.

projet, que nous représentons par le graphique ci-dessous. Il est ainsi attendu que les BTS CIEL alimentent majoritairement le parcours Cybersécurité de la Licence Informatique. Des actions de sensibilisation spécifiques seront de plus prévues aux différents niveaux de formation définissant le périmètre du projet, pour renforcer l'attraction vers les formations proposées dans le projet.



○ 1. 4. DIFFUSION DES DISPOSITIFS ET DES RESULTATS

L'élaboration et le déploiement d'un **plan de communication** autour des formations seront assurés au sein du Sous-WP 5. 3. Cela impliquera des activités de **promotion des formations proposées** sur les sites internets des partenaires, sur les plateformes nationales (notamment Mon Master) et sur le site web du GRETA-CFA de la Guadeloupe et des partenaires. Les actions de sensibilisation à destination des différents publics scolaires, professionnels et généralistes prévues au WP1 permettront également une diffusion de l'information autour de ces formations, notamment à travers des supports dédiés (brochures, flyers). Les partenaires du projet seront présents sur les **événements locaux d'orientation présentiels et en ligne**, notamment les Journées portes ouvertes de l'Université, le Salon de l'Orientation, de la Formation et des Métiers de Guadeloupe, le Salon virtuel de l'orientation de Guadeloupe, la Semaine de l'alternance, le Salon Formeo en Martinique ou encore le Forum des métiers à Saint-Barthélemy. Une démarche de **dissémination des résultats** sera conduite dans une volonté d'essaimage. Les études d'impact conduites sur le projet seront publiées aussi bien sur des canaux de communication grand public (sites internets des partenaires) qu'à travers des publications en sciences de l'éducation dans la lignée de la publication indiquée plus haut sur l'impact des pédagogies basées sur la réalité virtuelle. L'ACCYB pilotera l'animation d'une communauté de pratiques, et mobilisera le réseau en cours de mise en place au sein du Bassin Caraïbe (îles néerlandaises, Trinidad, Jamaïque).

● 2. ORGANISATION ET PILOTAGE DU PROJET

○ 2. 1. ORGANISATION DU CONSORTIUM

Le **modèle du pilotage du projet** aura 2 objectifs complémentaires : assurer le **suivi de la feuille de route du projet** pendant la période de financement et, de façon pérenne, garantir **la pertinence et l'actualisation des formations proposées**. Afin de répondre à ces deux objectifs, la gouvernance et le pilotage du projet seront proposés de la façon suivante :

Le **Comité de pilotage** sera **présidé par l'Université des Antilles** en tant que chef de file, et comprendra **un représentant de chaque partenaire** (ACCYB, GRETA-CFA de Guadeloupe, Rectorats de Guadeloupe et de Martinique, Orange Antilles-Guyane). Il définira la vision, la mission et les objectifs à long terme du projet et supervisera la mise en œuvre des activités. En plus de l'objectif direct qui est de créer conjointement une offre de formation d'excellence sur la cybersécurité aux Antilles, la mise en place de ce Comité de pilotage aura pour valeur ajoutée fondamentale de contribuer à la **structuration de l'écosystème public/privé autour de la cybersécurité sur ces territoires**. Il se réunira 1 fois par mois dans la première année du lancement projet, puis une fois tous les 3 mois une fois le dispositif pleinement installé.

○ 2. 2. PILOTAGE DU PROJET

■ 2. 2. 2. Dispositif de pilotage

Le Comité de pilotage sera secondé par une **équipe opérationnelle** qui comprendra le coordinateur et le responsable de qualité et communication qui seront recrutés spécifiquement, ainsi que les coordinateurs des work-packages. Cette équipe se réunira tous les mois.

De plus, le dispositif comprendra un **Conseil pédagogique et stratégique** réunissant des experts et parties prenantes désignés par le Comité de pilotage (p. ex. experts en cybersécurité, représentants des employeurs ou des filières, collectivités territoriales, membres de l'ANSSI). Ce Conseil instruira la démarche d'amélioration continue en assurant une veille sur les besoins en compétences sur l'évolution du secteur. Il réalisera une **étude de mi-parcours** sur l'évolution de la carte des formations en cybersécurité en lien avec le marché de l'emploi, ainsi qu'un **bilan final avec analyse d'impact.** Le projet sera mesuré au moyen d'un système d'indicateurs couvrant les aspects suivants[13] :

- **Sensibilisation** : %age de collèges et de lycées du territoire touchés par an, distribution sur les 4 îles du périmètre du projet, nb d'élèves touchés, nb de professionnels participant aux formations aux compétences de base, nb d'événements grand public organisés par an
- **Attractivité des parcours** : accroissement du nb de personnes attirées vers la filière à terme, accroissement du %age du public féminin au sein des formations
- **Formation** : nb de personnes formées par an en licence, nb de personnes formées par an en Master, nb d'inscrits au DU en cybersécurité par an, nb de certifications obtenues par an
- **Impact socio-économique** : tx d'insertion professionnelle, nb de reconversions professionnelles, nb de salariés accompagnés, nb d'emplois créés, nb d'entreprises créées offrant des services de cybersécurité, diminution du nb de cyberattaques, réduction du temps

[13] L'affinage du système d'indicateurs et la définition de cibles correspondante seront inclus dans la fiche de poste du responsable qualité recruté pour le projet

de gestion des incidents liés aux cyberattaques

- **Inclusivité du dispositif** : %age de public féminin parmi le public formé, %age de public féminin au sein de la formation de formateurs, %age de public touché au sein des territoires éloignés, nb de séniors touchés par le projet
- **Soutenabilité du dispositif** : revenus générés par le projet

■ 2. 2. 3. Calendrier de mise en œuvre

Année	Année 1				Année 2				Année 3				Année 4				Année 5			
Trimestre	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Work-package 1 : Sensibilisation et attraction vers la filière																				
Sous-WP 1.1. Déploiement d'équipements dans les trois Fab'Labs																				
Sous-WP 1.1. Mise en place d'ateliers de sensibilisation dans les Fab'Labs																				
Sous-WP 1.2. Ateliers Orange Digital Center																				
Sous-WP 1.2. Lancement du Serious Game Cyber																				
Sous-WP 1.2. Organisation d'un Hackathon Formation en cybersécurité																				
Sous-WP 1.3. Mise en place des modules de sensibilisation																				
Work-package 2 : Formation initiale en cybersécurité																				
Ingénierie pédagogique et élaboration des maquettes																				
Equipement des salles pour l'enseignement en hybride																				
Sous-WP 2.1. Lancement du parcours Cybersécurité de la licence Informatique																				
Sous-WP 2.2. Lancement du parcours Sécurité du numérique du M1 MIAGE																				
Sous-WP 2.2. Lancement du parcours Sécurité du numérique du M2 MIAGE																				
Work-package 3 : Formation continue en cybersécurité																				
Ingénierie pédagogique et élaboration des maquettes																				
Sous-WP 3. 1. Accompagnement des dirigeants et chefs d'entreprises																				
Sous-WP 3. 2. Création d'un Diplôme universitaire Cybersécurité																				
Sous-WP 3. 3. Préparation du Titre de Technicien Supérieur Système Réseaux																				
Work-package 4 : Formation de formateurs et soutien à l'insertion pro.																				
Sous-WP 4. 1. Formation des formateurs																				
Work-package 5 : Pilotage et communication																				
Sous-WP 5. 1. Mise en place des instances de pilotage et de l'équipe-projet																				
Sous-WP 5. 2. Suivi du projet et evaluation du dispositif																				
Sous-WP 5. 2. Etude de mi-parcours sur l'évolution de la carte des formations																				
Sous-WP 5. 3/4/5. Communication et promotion de la nouvelle offre de formation																				
Premiers retours d'expérience et adaptation du dispositif																				

○ 2. 3. PERENNITE DES DISPOSITIFS MIS EN PLACE

Les formations mises en place au sein du projet sont conçues de façon pérenne, et le financement demandé s'inscrit dans une démarche de **fonds d'amorçage**. Une partie des financements correspond à un **investissement initial** qui n'aura **pas besoin d'être réitéré** (ingénierie pédagogique, équipements, formation de formateurs). En plus de cela, le projet permettra de dégager progressivement des ressources, notamment à travers les **droits d'inscription** (DU) ou le renforcement des relations avec les entreprises. La labellisation CMA facilitera également l'attraction de ressources complémentaires (p. ex. Interreg, mécénat). Enfin, l'inscription dans le projet d'une **formation de formateurs** sert directement l'objectif de pérennisation du dispositif, en mettant en place un modèle vertueux en cascade pour le transfert de compétences.

En termes de **gouvernance**, le pilotage en mode projet cédera la place au terme de la période de financement à une gouvernance en continu visant à garantir en particulier la bonne évolution de la carte des formations. Le modèle définitif sera mis en place par le Comité de pilotage pendant la deuxième phase du projet, et les partenaires s'engagent à dédier les ressources requises pour ce modèle d'atterrissage.

● 3. JUSTIFICATION DES DEPENSES DU PROJET

CyberEDAntilles comporte un **coût total de 5 079 322 €** (hors frais d'environnement), dont **2 940 276 € (57,89 %)** sont demandés au titre de la subvention[14]. L'apport des partenaires s'élève à **2 139**

[14] Le budget a été revu à la baisse par rapport au montant indiqué dans la lettre d'intention pour tenir compte des remarques proposées par les évaluateurs.

046 €, répartis de la façon suivante (hors frais d'environnement) : UA - 609 272 € ; ACCYB - 256 360 €, GRETA-CFA Guadeloupe - 911 176 € ; Rectorat de Guadeloupe - 162 165 €, Rectorat de Martinique - 100 563 €, Orange Antilles-Guyane - 99 510 €. Le montant des **co-financements privés** (ACCYB et Orange Antilles-Guyane) est de **355 870** €. De plus, la **Collectivité territoriale de Martinique** et l'UA ont signé une Convention d'objectifs et de moyens 2023 - 2026, dont l'un des axes porte sur la construction d'une offre de formation avec co-financement à hauteur de 1,6M €. L'UA envisage de mobiliser une partie de ce financement à hauteur de **300 000 €** sur la période du projet qui viendront s'ajouter aux co-financements indiqués dans l'annexe financière.

Le budget du projet a été élaboré par un **calcul des coûts année par année**, avec un **modèle « en cloche »** : montée en puissance progressive (année 1 et 2), puis stabilisation et dégressivité en années 4 et 5 pour préparer l'absorption des coûts. Il intègre une **problématique de surcoûts** propres aux territoires ultramarins et au territoire antillais en particulier : projet qui couvre 2 régions académiques et 4 collectivités territoriales sur 2 835 km^2, ce qui engendre des **frais de déplacement** et d'équipement pour les modalités hybrides ; coûts liés à l'**importation des équipements** et à la **mobilisation de formateurs de l'Hexagone pour la formation de formateurs** ; surcoût de la **masse salariale** (indexation des salaires de 40%).

N°	Titre de l'action/de l'axe	Principaux postes de dépenses	Budget prévu (k€[15])	Aide demandée (k€)
1	WP1 sensibilisation et attraction vers la filière	Ingénierie pédagogique, indemnités intervenants experts et vacations, missions, supports de communication, encadrement administratif et pédagogique, équipements, fonctionnement événementiel	1142k€	610k€
2	WP2 Formation initiale	Ingénierie pédagogique, enseignements (vacation, enseignants contractuels, enseignements externalisés), encadrement administratif et pédagogique, équipements et maintenance (dont réalité augmentée, hybridation, laboratoire cyber), prestations de certification	2150k€	1203k€
3	WP3 Formation continue	Ingénierie pédagogique, enseignements (vacations, enseignants contractuels, enseignements externalisés via des prestataires), encadrement administratif et pédagogique, prestations de certification, équipements et matériel informatique	370k€	24k€
4	WP4 Formation de formateurs et insertion professionnelle	Formations de formateurs (prestations externalisées), budget de fonctionnement communication, missions	153k€	96k €

[15] Hors frais d'environnement et hors frais généraux.

5	WP5 Pilotage et communication	Recrutement coordinateur projet et responsable qualité et communication, participation partenaires aux instances du projet (coût RH et missions), budget de fonctionnement communication et participation à de l'événementiel sur les différentes îles (salons…), prestations intellectuelles pour le suivi de la cartographie formations	816k€	564k €

Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)

ANNEXE 2

REPARTITION DU BUDGET ENTRE ETABLISSEMENTS PARTENAIRES ET MOYENS MOBILISES

Nom du Responsable de projet : Université des Antilles

Identifiant Partenaire	Nom de l'établissement partenaire	Dotation financière	Fonds propres mobilisés
1	Université des Antilles	2 013 230,00 €	609 272 €
2	Lycée Les droits de l'homme – GRETA-CFA de la Guadeloupe	148 440,00 €	869 976 €
3	Rectorat de la Région Académique de la Guadeloupe	286 930,00 €	164 765 €
4	Agence Caribéenne pour la Cybersécurité	203 760,00 €	369 200 €
5	Orange Antilles Guyane	12 890,00 €	99 510 €
6	Rectorat de l'Académie de Martinique	0 €	99 823 €
7	GIP-FCIP Académie Martinique	234 750,00 €	0 €
TOTAL		**2 900 000 €**	**2 212 547 €**

Annexe 3 : Volet général du projet

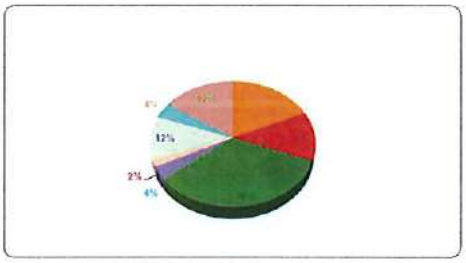
AMI - CMA	Réservé à l'organisme gestionnaire du programme	
	N° de partenaire	2023
	Acronyme	CyberEDAntilles
	Nb de partenaires	7
Document administratif et financier		Saison 2

Volet général
Fiche d'identité du projet

Acronyme du projet	CyberEDAntilles
Titre du projet	Enseignement et développement de la cybersécurité aux Antilles
Catégorie d'entité/Catégorie du bénéficiaire	Enseignement supérieur
Durée du projet (en mois) - max 60 mois	60
Date de démarrage souhaitée	Septembre 2024
Le projet prévoit une large diffusion des résultats et/ou une collaboration effective (au sens du RGEC) :	Oui

Equipements	22%
Prestations de service	14%
COED & COI	35%
Heures complémentaires	4%
Reconnaissance	2%
Missions	12%
Communication	6%
Frais généraux	17%

Répartition Aide demandée



Récapitulatif des demandes financières des partenaires

	Etablissement partenaire	Coût complet (comprenant les frais d'environnement, en €)	Coût complet (hors frais d'environnement, en €)	Total aide demandée (€)	Total assiette de l'aide (en €)	Assiette de l'aide, par catégorie de dépense (en €)								Apports hors frais d'environnement (en €)
						Equipements ou amortissement d'équipements de R&D	Prestations de service externes	% Prestations de service externes (max 30% assiette de l'aide, sauf dérogation)	Budget total Personnel AVEC financement demandé (€)	Heures complémentaires d'enseignement et modulation de service	Reconnaissance au titre des activités prévues au référentiel horaire	Missions	Autres dépenses externes (consommables, petits matériels ...)	Frais généraux	Total - Apports hors frais d'environnement (en €)
Part1-Coord	UA	2 922 324 €	2 622 502 €	2 013 330 €	2 013 230 €	312 623 €	57 000 €	2,83%	1 656 402 €	- €	- €	246 500 €	5 167 €	335 538 €	609 272 €
Part2	Collège RAIZET-GRETA	1 153 454 €	1 018 416 €	148 440 €	148 440 €	- €	82 500 €	55,58%	0 €	- €	- €	41 300 €	- €	24 740 €	869 976 €
Part3	RECTORAT GUADELOUPE	451 695 €	451 695 €	285 930 €	344 316 €	75 000 €	198 930 €	57,78%	0 €	- €	- €	13 000 €	- €	57 386 €	164 765 €
Part4	ACCYB	572 950 €	572 950 €	203 260 €	333 600 €	120 000 €	- €		0 €	- €	- €	50 000 €	113 600 €	56 600 €	369 200 €
Part5	ORANGE	112 400 €	112 400 €	12 890 €	51 559 €	9 600 €	37 872 €	73,45%	0 €	- €	- €	- €	- €	4 687 €	99 510 €
Part6	Rectorat Martinique	99 823 €	99 823 €	0 €	- €	- €	- €		0 €	- €	56 623 €	- €	- €	0 €	99 823 €
Part7	GIP-FCIP Académie Martinique	234 750 €	234 750 €	234 750 €	234 750 €	64 000 €	28 500 €	12,14%	0 €	116 944 €	- €	5 447 €	8 680 €	11 179 €	0 €
Totaux		5 547 415 €	5 112 546 €	2 900 000 €	3 331 895 €	580 623 €	404 802 €	12,93%	1 656 402 €	116 944 €	56 623 €	356 147 €	126 847 €	490 130 €	2 212 547 €

Assiette aide demandée frais généraux / Assiette aide demandée total hors frais généraux (max 20% sur l'ensemble du projet)	18,55%
Montant reconnaissance (limite annuelle de 50k€, sauf dérogation)	56 623 €
Aide totale demandée (en €)	2 900 000 €
Coût complet du projet (hors frais d'environnement, en €)	5 112 546 €
Coût complet du projet comprenant les frais d'environnement (en €)	5 547 415 €

Montant reconnaissance par an	11 325 €
Ratio Aide demandée / Coût complet du projet (hors frais d'environnement)	56,72%

	Taux d'aide demandé (%)		Sigle de l'établissement partenaire	Nom complet de l'établissement partenaire	N° de SIRET
Part1-Coord	100,0 %		UA	Université des Antilles	199 715 655 00011
Part2	100,0 %		Collège RAIZET-GRETA	Collège RAIZET - Greta de la Guadeloupe	199 714 056 00025
Part3	83,3 %		RECTORAT GUADELOUPE	RECTORAT DE LA REGION ACADEMIQUE DE LA GUADELOUPE	179 714 908 00033
Part4	60,0 %		ACCYB	Agence Caribéenne pour la Cybersécurité	918 214 890 00017
Part5	25,0 %		ORANGE	ORANGE ANTILLES GUYANE	380 129 866 00519
Part6	0,0 %		Rectorat Martinique	Académie de la Martinique	179 724 307 00030
Part7	100,0 %		GIP-FCIP Académie Martinique	GIP-FCIP Académie Martinique	189 723 056 00011

	Taux d'aide demandé (%)	WP 1	WP 2	WP 3	WP 4	WP 5	WP 6	WP 7	WP 8	WP 9	WP 10
Part1-Coord	100,0 %	0,00 €	1 093 362,00 €	0,00 €	32 000,00 €	552 333,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Part2	100,0 %	0,00 €	81 700,00 €	0,00 €	32 000,00 €	10 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Part3	83,3 %	105 666,62 €	0,00 €	0,00 €	23 333,31 €	10 833,33 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Part4	60,0 %	102 000,00 €	67 800,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Part5	25,0 %	11 718,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Part6	0,0 %	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
Part7	100,0 %	111 970,00 €	0,00 €	0,00 €	0,00 €	5 447,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €

NOTA : Toutes les champs de cet onglet "Volet général" doivent être renseignés.
Ils seront utilisés par les membres du jury au cours du processus de sélection.
Remarque : toutes les informations figurant ci-dessus ont vocation à être publiées si le projet est financé.
En déposant un dossier, les partenaires ont accepté la publication de toutes ces informations.

Responsable du projet

Prénom	Nom
Erick	STATTNER

Signature

Personne habilitée à engager l'établissement Chef de File

Prénom	Nom
Michel	GEOFFROY
Qualité	
Président	

Signature & Cachet

Le Président de l'Université des Antilles

Michel GEOFFROY

Recommandations : Une fois le document finalisé et imprimé, vérifier la présence de l'ensemble des signatures et cachets demandés avant de déposer la copie scannée en ligne.

Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)

ANNEXE 4

MEMBRES DU COMITE DE PILOTAGE

Nom du Responsable de projet : Université des Antilles

Identifiant Partenaire	Nom de l'établissement partenaire	Représentant	Fonction
1	Université des Antilles	Erick Stattner	Chef de file coordinateur
2	Lycée Les droits de l'homme – GRETA-CFA de la Guadeloupe	Valérie Géran	Directrice opérationnelle
3	Rectorat de la Région Académique de la Guadeloupe	Nicole Dupuy	Déléguée de région académique à la formation professionnelle initiale et continue (DRAFPIC)
		Corinne Flavier-Chaudrin	Adjointe à la DRAFPIC
4	Agence Caribéenne pour la Cybersécurité	Cédric Pradel	Directeur
5	Orange Antilles Guyane	Chantal Maurice	Directrice
6	Rectorat de l'Académie de Martinique	Sébastien Birbandt	Délégué de région académique pour le numérique éducatif (DRANE)
7	GIP-FCIP Académie Martinique	Olivier Chevillard	Directeur

Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)

ANNEXE 5

LISTE DES CONNAISSANCES PROPRES

Connaissances Propres : *Désignent les connaissances, informations, savoir-faire, secrets de fabrication, données, logiciels, méthodes et droits de propriété intellectuelle détenus par un Partenaire avant l'entrée en vigueur du présent Contrat ou développés en dehors du Projet (qui pourraient être utilisées dans le cadre du projet).*

Identifiant Partenaire	Nom de l'établissement partenaire	Liste des connaissances propres
1	Université des Antilles	
2	Lycée Les droits de l'homme - GRETA de la Guadeloupe	
3	Rectorat de la Région Académique de la Guadeloupe	
4	Agence Caribéenne pour la Cybersécurité	
5	Orange Antilles Guyane	
6	Rectorat de l'Académie de Martinique	
7	GIP-FCIP Académie Martinique	

ANNEXE 6

ORGANISATION DES RELATIONS ENTRE L'ACADEMIE DE LA MARTINIQUE ET LE GIP-FCIP DE L'ACADEMIE DE LA MARTINIQUE

OBJET

La présente annexe intervient en application de l'article 5 de l'accord de consortium.

Elle a pour objet de préciser les modalités de coopération entre L'académie de la Martinique (l'« Académie ») et le GIP-FCIP de l'académie de la Martinique (« le GIP-FCIP »), partenaires, dans la réalisation des travaux prévus par le projet CyberEDAntilles (le Projet) décrit en annexe « description du projet ».

L'Académie et le GIP-FCIP collaborent selon l'organisation décrite ci-dessous afin de permettre la bonne réalisation des actions prévues par ces deux partenaires dans le cadre du Projet.

REALISATION DES ACTIONS

1. PAR L'ACADEMIE

L'Académie :

- prépare et mobilise certains membres de son personnel pour construire et mettre en œuvre les actions pédagogiques attendues (Cf. annexe 2). Ce personnel mis à disposition du Projet est le suivant :
    - Les chargés de mission de la DRANE ;
    - Des enseignants ou autres personnels pédagogiques amenés à préparer les actions, après mise à niveau des compétences dans le domaine de la cybersécurité et de la ludopédagogie.
- assure la mise en œuvre des actions détaillées dans l'annexe 7 de la convention de consortium (Cf. annexe 2) conformément au Projet ;
- assure la coordination avec le GIP-FCIP, l'Université des Antilles et les autres partenaires du consortium ;
- assure la définition des actions, leur pilotage, la coordination de leurs acteurs et le suivi de leur réalisation, dont notamment : définition des besoins, recherche des intervenants, participation aux COPIL et missions, gestion du projet, organisation des actions et des formations, collecte des données, communication ;
- soutient le GIP-FCIP dans ses relations avec les établissements scolaires impliqués dans le Projet.

2. PAR LE GIP-FCIP

Le GIP-FCIP :

- assure le support et la gestion administrative et financière des actions détaillées dans l'annexe 7 du dossier de candidature (Cf. annexe 2), y compris leur exécution. Ceci inclut notamment : achat de prestations de services, achat d'équipements et paiement de vacations (formations, interventions pédagogiques) ;
- assure la gestion administrative et financière de l'ensemble des actions réalisées par l'Académie et le GIP-FCIP, en lien avec :
    - la directrice de la direction des affaires financières (DAFAP) de l'Académie, référente financière du projet pour l'Académie ;
    - la chargée de mission DRANE, référente pédagogique ;
    - la cheffe de projet CyberEDAntilles.
- soutient l'Académie dans l'animation et les échanges entre les différents acteurs du Projet et dans les actions mises en œuvre dans le cadre de celui-ci ;
- participe au développement et à la reconnaissance des compétences en cybersécurité des publics concernés par le Projet en favorisant leur accès à des parcours de formation, de validation des acquis de l'expérience ou des bilans de compétences.

GOUVERNANCE ET SUIVI

1. PILOTAGE

Un comité de suivi composé de représentants de l'Académie et du GIP-FCIP se réunit au minimum :

- Une fois par an pour faire le bilan des actions
- À la clôture du projet

Ce comité de suivi peut aussi se réunir ponctuellement, à la demande de l'une ou l'autre des parties.

2. RESPONSABLES DEDIES

Pour l'Académie : Sébastien BIRBANDT

Pour le GIP-FCIP : Olivier CHEVILLARD

3. PARTAGE D'INFORMATIONS

L'Académie et le GIP-FCIP transmettent l'un à l'autre toute information utile à la bonne exécution du Projet et à la justification de la réalisation des actions prévues. Ceci inclut notamment :

- feuilles d'émargement ;
- feuilles de temps ;
- lettres de mission ;
- Etc...

Le GIP-FCIP Transmet à l'Académie tous les éléments communiqués à l'Université des Antilles dans le cadre des reportings :

- Relevés de dépenses annuels au plus tard le 31 août de chaque année ;
- Indicateurs de suivi des actions ;
- Relevé final des dépenses au plus tard le 7 février 2030 ;

Le GIP-FCIP conserve tous les justificatifs de dépenses pendant 10 ans et tient une comptabilité séparée des dépenses liées au Projet.

L'Académie et le GIP-FCIP s'informent mutuellement, dans les meilleurs délais, de toute difficulté de mise en œuvre de leurs actions respectives dans le cadre du Projet.

Le

Pour l'académie,

ACADEMIE DE LA MARTINIQUE
RECTORAT
97279
SCHOELCHER
CEDEX

La Rectrice, Mme Nathalie MONS

Pour le GIP-FCIP,

GIP FCIP
Le Directeur
ACADEMIE DE MARTINIQUE

Le Directeur, M. Olivier CHEVILLARD

Avenant n°1

A LA CONVENTION DE REVERSEMENT DE FONDS
Université des Antilles/ACCYB

Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)

ENTRE

L'Université des Antilles
Etablissement public à caractère scientifique, culturel et professionnel (EPSCP)
Référencée sous le numéro SIRET 199 715 855 00011
Située au Campus de Fouillole, BP 250, 97175 Pointe-à-Pitre, Guadeloupe

Représentée par son Président, Monsieur Michel GEOFFROY

Ci-après dénommée par « UA » ou « le Chef de file »

D'une part,

ET

Association Agence Caribéenne pour la Cybersécurité (ACCYB),
Association enregistrée au registre des associations W9G1011279 au Code APE 94.99Z
Référencée sous le numéro SIRET : 918 714 890 00012
Située 189 rue Victor Mamado, 97128 Goyave, Guadeloupe

Représenté par son Président, Monsieur Steven COCKS

ci-après dénommée par « ACCYB » ou « le partenaire »

D'autre part,

PRÉAMBULE
La Convention de reversement de fonds conclue entre les Parties- le 13 février 2026 fixe les modalités de reversement de l'aide attribuée dans le cadre du projet CyberEdantilles.
Il a été constaté une erreur matérielle dans la rédaction de l'Article 6 relatif au montant maximal de la quote-part attribuée à l'Établissement partenaire.
Par ailleurs, le changement de présidence intervenu au sein de l'Établissement partenaire induit une erreur matérielle dans la désignation du représentant légal au sein de ladite convention.

Les Parties ont en conséquence convenu d'établir le présent avenant rectificatif afin de corriger ces éléments, sans modifier l'économie générale de la convention initiale.

ARTICLE 1 – OBJET DE L'AVENANT
Le présent avenant a pour objet :
- d'actualiser la désignation du représentant légal de l'Établissement partenaire ;
- de modifier l'article 6 de la convention précitée.

ARTICLE 2 – MODIFICATION DE LA REPRÉSENTATION DE L'ÉTABLISSEMENT PARTENAIRE
La Convention de reversement signée le 13 février 2026 mentionne l'Etablissement partenaire représenté par sa Présidente, Madame Marie-Lucienne Rattier.

Cette mention induit une erreur.

L'Établissement partenaire est représenté par son Président, Monsieur Steven Cocks, tel qu'entériné lors de l'assemblée générale en date du 4 février 2026.

Les stipulations de la Convention doivent être lues en conséquence.

ARTICLE 3 - MODIFICATION DE L'ARTICLE 6
L'Article 6 – Montant de l'aide et modalités de reversement est remplacé par les dispositions suivantes :

ARTICLE 6 – MONTANT DE L'AIDE ET MODALITÉS DE REVERSEMENT
Sous réserve de la mise à disposition effective des fonds au Chef de file, de l'absence de mise en œuvre de l'article 8 de la Convention et du respect par l'Établissement partenaire de ses obligations contractuelle, le Chef de file s'engage à verser à l'Établissement partenaire une quote-part de l'aide d'un montant maximal de **203 760,00 € (deux cent trois mille sept cent soixante euros)** selon les modalités prévues par la convention.

ARTICLE 4 – DISPOSITIONS FINALES
Toutes les autres stipulations de la Convention demeurent inchangées et continuent de produire leurs effets.
Le présent avenant entre en vigueur à la date de sa signature par l'ensemble des Parties.

En 2 exemplaires originaux

Pour l'ACCYB	Pour l'UA
Le : 20/03/2026	Le :
Le Président	**Le Président**
Cocks Steven	
Steven COCKS	**Pr Michel GEOFFROY**

APPEL A MANIFESTATION D'INTERET COMPETENCES ET METIERS D'AVENIR - CMA 2023

CATEGORIE : DISPOSITIF DE FORMATION

DOCUMENT PRESENTATION PROJET

CyberEDAntilles

Acronyme	CyberEDAntilles	
Titre du projet	Enseignement et développement de la cybersécurité aux Antilles	
Chef de file	**Raison sociale, structure juridique et N° Siret**	
	Université des Antilles, EPSCP, SIRET 19971585500011, Département 971 (Guadeloupe)	
Responsable du projet	**Nom, prénom et fonction**	
	Pr Erick Stattner Professeur des Universités en Informatique, Université des Antilles, Directeur Département Mathématiques-Informatique (DMI)	
	Courriel	**Téléphone**
	erick.stattner@univ-antilles.fr	Bureau: +(590) 590 48 34 31 Gsm. : +(596) 696 95 32 00
Durée du projet (max 60 mois)	**60 Mois**	
Aide totale demandée	**2 940 276 €**	
Coût total du projet	**5 079 322 € (hors frais d'environnement)** **5 522 257 € (avec frais d'environnement)**	
Merci de cocher le(s) volet(s) de l'AMI CMA concerné(s) par votre projet	☑ Les dispositifs transversaux d'attractivité et d'innovation ☑ Les voies d'excellence professionnelles et technologiques ☑ Les voies d'excellence académiques : ☑ Formation postbac, ☑Formation master, doctorat, attractivité internationale ☑ L'accompagnement des parcours professionnels	
Merci de cocher les secteur(s) éligible(s) aux priorités France 2030 (voir annexe 3 du cahier de charges de l'AMI - CMA)	**Faire émerger des réacteurs nucléaires de petite taille, innovants et avec une meilleure gestion des déchets** ☐ Nucléaire	

	Devenir le leader de l'hydrogène vert et des énergies renouvelables ☐ Devenir le leader de l'hydrogène vert **Décarboner notre industrie** ☐ Décarbonation de l'industrie ☐ Electronique et robotique ☐ Recyclabilité, recyclage et réincorporation de matériaux recyclés ☐ Technologies avancées pour les systèmes énergétiques ☐ Produits biosourcés et biotechnologies industrielles, carburants durables ☐ Solutions pour la ville durable et bâtiment innovant **Produire en France, à l'horizon 2030, près de 2 millions de véhicules zéro émission chaque année et développer une mobilité sobre, souveraine et résiliente** ☐ Véhicules connectés zéro émission ☐ Digitalisation et décarbonation des mobilités ☐ Batteries **Produire le premier avion bas carbone** ☐ Avion bas carbone **Investir dans une alimentation saine, durable et traçable afin d'accélérer la révolution agricole et alimentaire** ☐ Alimentation saine, durable et traçable ☐ Systèmes agricoles durables et équipements agricoles contribuant à la transition écologique **Produire 20 biomédicaments contre les cancers, les maladies chroniques dont celles liées à l'âge et créer les dispositifs médicaux de demain** ☐ Produire 20 biomédicaments ☐ Santé numérique ☐ Maladies infectieuses (ré)émergentes et menaces NRBC **Placer la France à nouveau en tête de la production des contenus culturels et créatifs** ☐ Industries créatives et culturelles **Prendre toute notre part à la nouvelle aventure spatiale**

	☐ Aventure spatiale **Investir dans le champ des fonds marins** ☐ Fonds marins **Souveraineté numérique** ☐ 5G et futures technologies de réseaux de télécommunications ☐ Cloud ☐ Intelligence artificielle ☐ Technologies du quantique **☑ Cybersécurité** ☐ Verdissement du numérique **Dispositifs transversaux d'innovation et d'attractivité** ☐ Enseignement et numérique ☐ Attractivité
Zone géographique de couverture du dispositif de formation (Veuillez préciser la/les région(s) visées)	• Guadeloupe • Martinique • Saint-Barthélemy • Saint-Martin
Type(s) de formation envisagé(s)	**☐ Scolaire ☑ Supérieur** **☑ Formation continue ☑ Sensibilisation**
Formation(s) / Titre(s) / Certification(s) visé(s)	• Licence informatique parcours Cybersécurité • Master MIAGE parcours Sécurité du numérique • Diplôme universitaire Cybersécurité • Titre de Technicien Supérieur Système Réseaux - option cybersécurité • Certification ISO 27001 • Certificat national CléA numérique • Accompagnement de dirigeants et chefs d'entreprise • Actions d'attraction vers la filière et de sensibilisation • Formation de formateurs en cybersécurité
Indiquer les sites sur lesquels les formations CMA seront publiées pour informer le public d'apprenants ciblés.	• Site internet de l'Université des Antilles • Site internet du GRETA-CFA de la Guadeloupe • Site internet du CARIF-OREF de la Guadeloupe • Plateforme nationale Mon Master • Salon virtuel de l'orientation en Guadeloupe
Branche(s) professionnelle(s) concernée(s) (si pertinent)	Personnel des prestataires de services du secteur tertiaire
Suite d'un projet CMA « Diagnostic »	**☑ Non ☐ Oui, préciser :**

Projets précédemment financés par le PIA ou France 2030	**☑ NON ☐ OUI, préciser :** **☐ *CMQe* ☐ *EUR* ☐ *IDEFI* ☐ *NCU*** **☐ *IFPAI* ☐ *PFPE*** **☐ *Autre* : ……**
Mots-clefs (1)	1. Cybersécurité 2. Antilles 3. Attraction et sensibilisation 4. Formations universitaires 5. Formation de formateurs 6. Alternance 7. Professionnalisation 8. Écosystème public-privé 9. Continuum pré-bac/post-bac 10. Hygiène numérique

(1) *Les expressions suivantes, trop génériques, ne sont pas permises :* FI, FC, FTLV, formation initiale, formation continue, formation tout au long de la vie, formation, compétences, métiers, innovation, transformation, pédagogie, outils pédagogiques innovants, enseignement scolaire, enseignement supérieur, entreprises.

LISTE DES MEMBRES DU CONSORTIUM (SI CONSORTIUM) – FOURNIR RAISON SOCIALE, STRUCTURE JURIDIQUE, N° SIRET ET N° DEPARTEMENT DE L'ÉTABLISSEMENT (cf. cahier des charges)

Organismes de formation ou d'accompagnement (universités, écoles, lycées, CFA, CFPPA, organismes privés, Pôle emploi/France Travail, associations, etc.).	***Secteur(s) d'activité***
Chef de file : Université des Antilles - EPSCP	Université, SIRET 19971585500011, Département 971 (Guadeloupe)
GRETA-CFA de la Guadeloupe	Groupement d'établissements publics locaux d'enseignement de l'Éducation Nationale, SIRET 19971405600025, Département 971 (Guadeloupe)
Agence caribéenne pour la cybersécurité	Association loi 1901, SIRET 91871489000012, Département 971 (Guadeloupe)

Donneurs d'ordre publics dans l'achat de formation (conseils régionaux, Pôle emploi/France Travail, OPCO,etc.)	***Secteur(s) d'activité***
Rectorat de la Région académique de Guadeloupe,	Rectorat, SIRET 17971430800238, Département 971 (Guadeloupe)
Rectorat de la Région académique de Martinique,	Rectorat, SIRET 1797243000030, Département 972 (Martinique)

Employeurs ou leurs représentants (entreprises, groupements d'employeurs, comité stratégique de filière, organisations professionnelles, syndicats, fédérations professionnelles , etc.)	***Secteur(s) d'activité***
Orange Antilles Guyane, Société anonyme	Entreprise secteur Télécoms, SIRET 38012986600519, Département 971 (Guadeloupe)

Recueil d'indicateurs à compléter de manière obligatoire sur le site de soumission CMA :

*Sur le site de soumission, vous devrez compléter de manière obligatoire l'onglet « **Informations Formations** ». Il s'agit d'un recueil d'indicateurs sur les formations envisagées dans le cadre votre projet, sur toute la durée du projet.*

Résumé du projet (Non confidentiel – 4000 caractères maximum, espaces inclus)

CyberEDAntilles est un dispositif ambitieux de formation initiale et continue en cybersécurité à destination du territoire antillais (Guadeloupe, Martinique, Saint-Barthélemy, Saint-Martin). Porté par l'Université des Antilles en collaboration avec un ensemble d'acteurs publics et privés, il a été élaboré sur la base d'un diagnostic révélant :

- des **lacunes dans l'offre de formation initiale et continue en cybersécurité**, générant un **déficit de compétences locales** ;
- une **forte vulnérabilité** aux cyberattaques, aussi bien pour les organisations publiques (collectivités) que pour les PME et TPE ;
- un **déficit de compétences et d'experts sur le territoire** pour répondre aux cybermenaces et participer aux actions de formations ;
- un **manque d'attractivité de la filière**, qui comporte pourtant un fort potentiel d'insertion professionnelle sur des territoires très touchés par le chômage ;
- l'importance d'une démarche de **formation de formateurs en cybersécurité** pour renforcer la souveraineté numérique du territoire.

Pour y répondre, CyberEDAntilles propose un **bouquet complet de formations** sur un continuum **du pré-bac à la formation supérieure et continue** pour développer des compétences expertes en matière de cybersécurité, ainsi que des **actions de sensibilisation** visant à renforcer le niveau de sécurité global du territoire. Il est articulé en **5 works-packages** :

1. **Sensibilisation et attraction vers la filière** : sensibilisation, acculturation et formation aux compétences de base vers les publics scolaires, les étudiants de l'Université et le grand public
2. **Formation initiale** : création d'un parcours « Cybersécurité » au sein de la Licence Informatique et d'un parcours « Sécurité du numérique » au sein du Master MIAGE
3. **Formation continue** : création d'un Diplôme universitaire Cybersécurité, préparation du Titre de Technicien Supérieur Système Réseaux - option cybersécurité, accompagnement des dirigeants et chefs d'entreprise
4. **Formation de formateurs et soutien à l'insertion professionnelle**
5. **Pilotage et communication**

Ces actions seront déployées par un **consortium multi-acteurs** réunissant l'**Université des Antilles**, les **Rectorats de Guadeloupe et de Martinique** (actions vers les publics scolaires) ; le **GRETA-CFA de Guadeloupe** (formation continue), l'**Agence caribéenne pour la cybersécurité**, (sensibilisation et la communication) ; **Orange Antilles-Guyane** (programme Orange Digital Center pour conduire une démarche de sensibilisation notamment vers les publics fragiles).

Le projet est également soutenu par un **réseau d'organisations souhaitant appuyer son déploiement**, par exemple en accueillant des apprentis ou en participant à la veille sur les besoins en compétences : Association du Numérique du Secteur Public, Chambre Économique Multiprofessionnelle de Saint-Barthélemy, CLUSIR, EXODATA, France Travail, Gendarmerie

nationale, Réseau CANOPE, OPCO AFDAS, UDE-MEDEF, collectivités territoriales (actions également envisagées avec le CNFPT et l'OPCO AKTO).

CyberEDAntilles mobilisera des **pédagogies innovantes** particulièrement adaptées à un contexte multi-insulaire, telles que des modalités hybrides et un recours à la réalité virtuelle. Les formations initiales et continues seront proposées en **alternance**, d'une façon qui favorisera l'insertion professionnelle et les interactions public-privé autour de la cybersécurité aux Antilles.

CyberEDAntilles sera déployé sur **5 ans**. Le coût complet du projet est de 5 079 322 €, dont 2 940 276 € de demande France 2030, et 2 139 046 € d'apport des partenaires. Il sera piloté par un **Comité de pilotage** assisté d'une **équipe opérationnelle** et d'un **Conseil pédagogique et stratégique**.

En répondant à un besoin avéré de création de compétences locales, CyberEDAntilles exercera un **impact mesurable sur la compétitivité de l'économie territoriale**, tout en renforçant la souveraineté numérique dans un Bassin marqué par une forte concurrence internationale.

Sommaire

1. DESCRIPTION DU PROJET DE DISPOSITIF(S) DE FORMATION ET D'ATTRACTIVITE

1. 1. PRESENTATION DU CONTEXTE

Dans une tribune récente[1], Bruno Bonnell, secrétaire général pour l'investissement en charge de France 2030, souligne l'**urgence du besoin de formations en cybersécurité**, dans un contexte marqué par une augmentation de plus de 37 % du nombre de cyberattaques entre 2020 et 2021 selon l'Agence nationale de la sécurité informatique (ANSSI). Comme le souligne cette tribune, cela exige « de décloisonner les filières dans l'informatique et de chasser l'*a-priori* voulant que la cybersécurité soit réservée aux techniciens et ingénieurs ».

CyberEDAntilles - Enseignement et développement de la cybersécurité aux Antilles répond directement à ce **besoin de formations plurielles en cybersécurité** aux Antilles françaises. Il a été élaboré sur la base d'un **diagnostic approfondi** concernant les **formations existantes** en Martinique et de Guadeloupe, les **compétences demandées sur le marché de l'emploi** et l'**incidence des cyberattaques** sur le territoire antillais. Ce diagnostic a été élaboré conjointement par l'Université des Antilles (UA), le Rectorat de la Guadeloupe, les DEETS Guadeloupe et Martinique, l'Agence caribéenne pour la cybersécurité et la Gendarmerie nationale.

Rôle des établissements d'enseignement supérieur dans la stratégie française cybersécurité : extrait de l'éditorial par Vincent Strubel, Directeur général de l'ANSSI, Sécurité des SI : La cybersécurité au cœur de la stratégie de l'ESRI (fév. 2024)

> A la veille de la transposition de la directive NIS 2 en droit français qui oblige les Etats membres à adopter une stratégie nationale concernant l'éducation et la formation, la recherche et le développement en matière de cybersécurité[1], nous encourageons les ESRI à se mobiliser afin qu'ils développent une plus grande **culture de la gestion du risque cyber et s'approprient les objectifs de cybersécurité** à atteindre. La France a besoin de s'appuyer sur des générations diplômées et acculturées au risque cyber.

En particulier, l'UA et le Rectorat de Guadeloupe sont parties prenantes des **travaux relatifs à l'EDEC numérique lancés par la DEETS Guadeloupe**[2], qui aboutiront à la mise en place d'un plan de formation coordonné. Les fiches prospectives proposées pour les différentes branches professionnelles révèlent en effet que la Guadeloupe est perçue comme un **territoire vulnérable aux risques cyber**, avec un niveau de compétences variable selon les acteurs, et un besoin réel d'accompagnement, notamment pour les **TPE/PME** dont est principalement composé le tissu économique du territoire. Dans de nombreux secteurs, il est essentiel de mettre en place un **socle de compétences techniques et transverses en matière de cybersécurité et de sécurisation des données**, ainsi qu'une **formation de professionnels de la cybersécurité** (techniciens cybersécurité, Data Protection Officers, consultants cybersécurité, analystes/techniciens Security Operations Center...). Par ailleurs, le diagnostic souligne un **manque d'attractivité** pour les métiers de la cybersécurité en Guadeloupe, en raison d'un décalage entre l'image et la réalité du métier, d'un manque de passerelles avec d'autres métiers et d'une offre de formation jugée inadéquate par les professionnels. C'est pourquoi il recommande d'« **intégrer les compétences techniques et transverses de cybersécurité dans les cursus des formations initiales en Numérique**, développer une **offre certifiante** et des **passerelles** sur les métiers spécifiques à la cybersécurité, accessible à niveau Bac+2 ou Bac+3 (...), créer des **passerelles entre les métiers de la cybersécurité et les métiers du réseau** (administrateurs systèmes et réseaux) ».

En **Martinique**, le Contrat d'Étude Prospective Métiers du Numérique (conclusions préliminaires - janvier 2024) démontre également d'importantes opportunités de développement économique dans

[1] Tout le monde peut travailler dans la cybersécurité !, La Tribune, novembre 2023.
[2] Source : EDEC Numérique Guadeloupe DEETS-AKTO/ATLAS.

le secteur de la cybersécurité, mais aussi une structuration insuffisante de la formation.

Cybersécurité en Martinique : Opportunités	Cybersécurité en Martinique : Faiblesses
Nouvelles **opportunités de marché** Levier pour le développement du **commerce en ligne** Stratégie de mise en place d'un **territoire souverain numériquement** Devant le risque accru de cyberattaque, les **commissaires aux comptes** vont demander de faire des provisions pour le risque cyber Les **assurances** vont mettre en place des questionnaires très précis sur les actions cybersécurité menées par les entreprises et en fonction de la criticité de leurs activités, décideront de les assurer ou non.	**Lacunes de l'offre de formation : Difficultés de recrutement niveau ingénieur/Bac+5**, problèmes d'adaptation des ingénieurs de l'Hexagone, les **titulaires d'un BTS ou DUT** qui souhaitent poursuivre en étude d'ingénieurs doivent partir se former en dehors, une **offre de formation continue** qui fait défaut, au sein de l'**Université des Antilles** : Licence informatique générale, mais pas de module cybersécurité **Difficulté à trouver de bons formateurs** **Manque de compétences au sein du tissu entrepreneurial et manque d'anticipation** : les chefs d'entreprise doivent être formés aux risques de cyberattaques et incités à la **réalisation d'audit et l'analyse des risques** **Concurrence internationale** au sein du Bassin
Recommandations	
Création de formations spécifiques à la cybersécurité : auditeur, chef de projet cybersécurité, architecte cybersécurité, formations certifiantes (ANSSI), modules cybersécurité au sein de formations transverses... **Actions de sensibilisation et d'acculturation** sur la digitalisation et la cybersécurité Mise en place de **formations continues sur la cybersécurité** Continuer à développer l'**alternance** Rendre la **formation professionnelle** plus lisible, plus accessible **Mise en avant de certains métiers** : RSSI, chef de projet Cyber, Architecte Cloud-Cyber… **Plus forte intégration dans les formations des enjeux cybersécurité** et de transition environnementale Mettre en place une **formation de formateurs**.	

Si des formations courtes pré ou post-bac en cybersécurité ainsi qu'une offre de formation privée existent en Guadeloupe et en Martinique[3], il y a aujourd'hui un manque de **formations expertes de niveau licence ou Master**, ainsi qu'au niveau de la **formation continue**. L'offre est par ailleurs dispersée et peu lisible, et il n'existe pas à ce jour de **dispositif intégré** proposant un **bouquet complet de formations** avec une identité thématique sur l'ensemble du continuum depuis le pré-bac jusqu'au post-bac et à la formation continue. Il existe pourtant un **potentiel à la fois en termes de vivier étudiant et de personnel enseignant**, puisque l'UA propose notamment une licence en informatique, ainsi qu'un Master Informatique et un Master Méthodes Informatiques Appliquées à la Gestion des Entreprises (MIAGE). Cependant, comme le souligne le diagnostic cité plus haut,

[3] Guadeloupe : Bac Pro CIEL, Mention complémentaire Cybersécurité ; BTS cybersécurité, informatique et réseaux, électronique option A informatique et réseaux ; Plateforme privée de formation numérique Concept X Formation, Certifications proposées par des opérateurs privés (M2i, Webforce3), Modules proposés par le CNAM Guadeloupe et par la CCI Guadeloupe. Martinique : Bac Pro CIEL, Mention complémentaire Cybersécurité ; BTS cybersécurité, informatique et réseaux, électronique option A informatique et réseaux ; BTS Services Informatiques aux Organisations, option SISR en alternance (CCI Martinique et CFA Skillfor) ; Métiers des Réseaux Informatiques et Télécommunications parcours Administration et Sécurité des Systèmes - 3ème année (CCI Martinique et CFA Skillfor) ; L3 STS mention Informatique Générale option Cybersécurité (CNAM Martinique) ; Modules de formation continue proposés par le CNAM Martinique ; Modules de formation continue proposés par des organismes privés (M2i, Unichrone).

l'Université ne propose pas de formations spécifiques en cybersécurité[4], et les jeunes souhaitant se spécialiser doivent donc soit se tourner vers des opérateurs de formation privés, soit aller étudier dans l'Hexagone, ce qui génère des inégalités territoriales.

Le développement d'une telle offre de formation est d'autant plus fondamental que **le territoire antillais a fait l'objet de nombreuses cyberattaques** au cours des dernières années : LADOM en 2015, plusieurs dizaines de TPE/PME en Guadeloupe en 2020, Collectivité Territoriale de Martinique en 2022-2023, Conseil régional de la Guadeloupe en novembre 2022, puis nouvelle cyberattaque par des hackers pro-russes en février 2024. La capacité à lutter efficacement contre ces menaces requiert le développement de **compétences internalisées** et une formation à l'identification des menaces au sein du Bassin caribéen et de son environnement international.

En France, le secteur de la cybersécurité est par ailleurs un **secteur en tension**, avec **15 000 postes non pourvus**, et environ **37 000 postes qui devraient être créés à horizon 2030**[5]. La Stratégie nationale d'accélération sur la cybersécurité se donne quant à elle pour objectif de passer de 37 000 à 75 000 emplois en cybersécurité à Horizon 2025[6]. Ces besoins s'accroîtront avec différents facteurs comme le **passage à la facturation électronique obligatoire**, ou encore le **Cyber Resilience Act** et la **Directive NisV2** adoptée par l'Union européenne qui renforce les règles en matière de cybersécurité. Cela implique une **insertion professionnelle** importante, et des **conditions attractives** avec un salaire d'entrée souvent plus élevé que la moyenne. Cette opportunité est particulièrement valorisante dans le contexte antillais, puisque **27% des jeunes de 15 à 29 ans en Guadeloupe ne sont ni en emploi, ni en études, ni en formation**[7], et que ce pourcentage est de **26% en Martinique**[8], soit deux fois plus que dans l'Hexagone.

Profil type d'un professionnel de la cybersécurité

- Un homme
- De 30 à 49 ans
- De niveau de qualification Bac +5
- Issu du domaine informatique/numérique
- De moins de 10 ans d'expérience dans la cybersécurité
- Travaillant en Ile-de-France
- Salarié du secteur privé
- Travaillant au sein d'une équipe de professionnels de la cybersécurité
- Travaillant dans une structure de 1 000 salariés et plus
- Travaillant dans une structure non spécialisée en cybersécurité
- Consultant cybersécurité ou RSSI
- 100% de son temps est consacré aux questions de cybersécurité
- Plutôt recruté via le marché caché
- Régulièrement sollicité par des recruteurs

Afin de faciliter la création d'emplois et de diversifier les profils, il est fondamental de travailler sur l'**attractivité de cette filière**. L'enquête réalisée par l'ANSSI en 2021 sur les Profils de la cybersécurité révèle en effet un profil souvent monolithique en cybersécurité, qu'il serait intéressant d'ouvrir davantage vers un public féminin, plus jeune, ouvert aux formations courtes et aux compétences transversales, éloigné des grands centres métropolitains, susceptible d'être employé par le secteur public et/ou dans un environnement économique composé en grande partie de TPE et de PME.

○ 1. 2. DESCRIPTION DU OU DES DISPOSITIFS DE FORMATION ET/OU D'ATTRACTIVITE

■ 1. 2. 1. Les métiers et compétences

De par son large spectre d'intervention, CyberEDAntilles permettra aussi bien de former des **publics de formation initiale et continue** sur des métiers spécifiques au domaine de la cybersécurité que de garantir un **socle de compétences** en cybersécurité au sein de **métiers aux interfaces**. Les

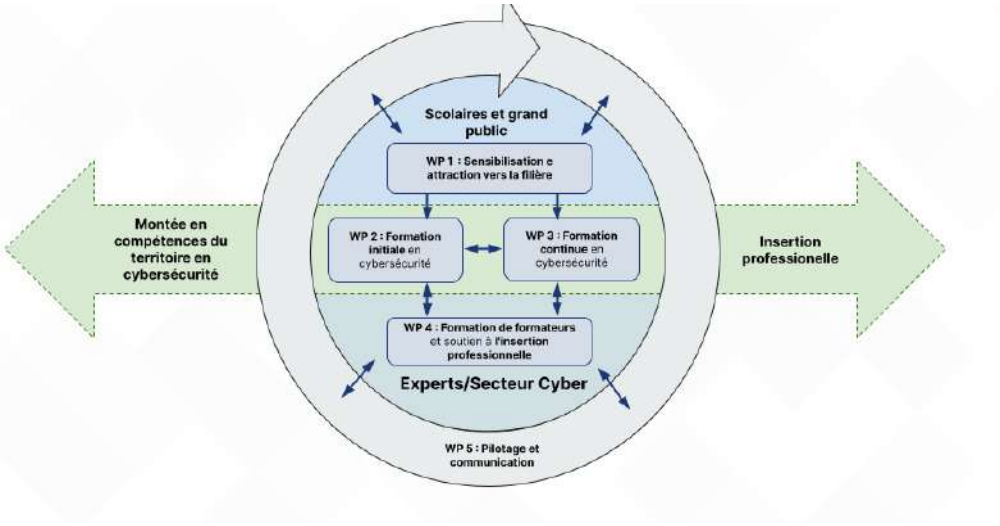
[4] Un projet de formation avait été accrédité en 2018 mais n'avait pas abouti faute d'enseignants spécialistes.
[5] Cybersécurité : où en sont les grandes entreprises françaises, Wavestone, 2022.
[6] Source : Communiqué de presse du Gouvernement.
[7] Source : INSEE.
[8] Source : INSEE.

métiers directement liés aux compétences clés de la cybersécurité seront notamment : Administrateur système/réseau/base de donnée ; Administrateur d'infrastructures sécurisées ; Responsable de la sécurité des systèmes d'information ; Consultant en sécurité informatique ; Architecte systèmes et logiciels ; Ingénieur en Cybersécurité ; Technicien Supérieur Système Réseaux ; Responsable de la sécurité des systèmes d'information ; Consultant en sécurité informatique.

L'acquisition de **socles de compétences** en cybersécurité permettra également aux professionnels formés d'aborder les problématiques de sécurité du numérique dans des domaines variés, par exemple Banque - finance - assurance, Administration, Économie - comptabilité - gestion - finances, Industrie - qualité - gestion des risques, Informatique - télécommunication, Marketing - commerce - distribution, Médias - communication - audiovisuel, Numérique - multimédia - web, Ressources humaines - management, Santé, Social ou encore Transport.

En formant non seulement des futurs professionnels de la cybersécurité, mais en développant des compétences transversales utiles dans tout un ensemble d'autres secteurs, CyberEDAntilles répond aux enjeux du développement des compétences numériques, qui sont ceux d'une transformation de l'ensemble de l'économie à travers ce levier.

■ 1. 2. 2. Le projet



Périmètre et consortium : CyberEDAntilles propose un bouquet de formations à destination d'un continuum allant du **public pré-bac** (sensibilisation et attraction vers la filière) au **public post-bac de la formation initiale**, **l'alternance et la formation continue**. Elles s'adresseront en premier lieu au **public du territoire antillais** (Guadeloupe, Martinique, St-Barthélémy, St-Martin), mais seront également ouvertes à un **public plus large au sein du Bassin caribéen** (p. ex. : Sint Maarten). Les enjeux de souveraineté nationale sont particulièrement marqués au sein du Bassin compte tenu de la présence proche de l'industrie nord-américaine, renforçant l'importance d'une structuration à l'échelle du Bassin au service du rayonnement de la France dans la région.

CyberEDAntilles est proposé par un **consortium** ambitieux réunissant des acteurs publics de la formation initiale et continue, ainsi que des acteurs privés territoriaux. Il est porté par l'**Université des Antilles**, établissement-phare de l'enseignement supérieur aux Antilles, et comprend des représentants des employeurs (**Orange Antilles-Guyane**), des organismes de formation et d'accompagnement (**GRETA-CFA de Guadeloupe, Agence caribéenne de cybersécurité**) et des donneurs d'ordre publics dans l'achat de formation continue des chercheurs d'emploi (**Rectorats de Guadeloupe et de Martinique**). CyberEDAntilles a de plus constitué un **réseau d'organisations publiques et privées** exprimant l'intention d'en faciliter le déploiement, par exemple en accueillant des apprentis ou en contribuant à la veille sur les besoins en compétences : Association du Numérique du Secteur Public, Chambre Économique Multiprofessionnelle de Saint-Barthélemy,

CLUSIR, EXODATA, France Travail, Gendarmerie nationale, Réseau CANOPE, OPCO AFDAS (actions également envisagées avec l'OPCO AKTO et le CNFPT), UDE-MEDEF. La Collectivité territoriale de Martinique est associée au projet. La Région Guadeloupe le sera également, notamment via l'Agence Caribéenne pour la Cybersécurité et le Rectorat de Guadeloupe.

Structuration du projet

CyberEDAntilles est pleinement aligné avec la **Stratégie Nationale Cyber**, et notamment avec son **Axe 4 - Former plus de jeunes et professionnels aux métiers de la cybersécurité**. Il a été conçu en adéquation étroite avec les attendus de la fiche thématique Cybersécurité, qui formule deux priorités :

- **Former davantage de personnes aux métiers de la cybersécurité incluant toutes les déclinaisons de niveau de spécialisation** en fonction des postes visés pour répondre à la très forte demande en compétences du secteur et soutenir sa croissance
- **Former le plus grand nombre aux enjeux, dangers et gestes simples de la cybersécurité** à la fois pour soutenir la demande mais aussi, et surtout, pour élever le niveau de sécurité global du pays

Pour relever ces deux défis, CyberEDAntilles se déploie en **5 work-packages** présentés ci-après.

Work-package 1 : Sensibilisation et attraction vers la filière
Objectifs - Attraction des jeunes/des publics scolaires vers les formations en cybersécurité, avec un focus sur les publics éloignés (notamment public féminin) - Acculturation et initiation aux compétences de base en cybersécurité dans des secteurs transverses - Élévation du niveau de compétences en cybersécurité au service d'une transformation de l'économie
Description des actions **Sous-WP 1. 1. Attraction vers la filière au collège (3ème) et au lycée**, en partenariat avec les Rectorats de Guadeloupe et de Martinique. En Guadeloupe, l'Académie dispose de 9 Fab'Labs équipés et aménagés par les collectivités (Région Guadeloupe et Collectivité de Saint-Martin) dans 9 lycées répartis sur le territoire. La sensibilisation sera menée à travers 2 types d'ateliers dispensés en priorité au sein de ces Fab'Labs : ateliers de sensibilisation pour les élèves de 3ème et 2nde et ateliers avancés de sensibilisation pour les élèves de Terminale et de BTS. Les enseignants bénéficieront des ressources de CANOPE Guadeloupe[9] pour la sensibilisation à la cybersécurité et à l'hygiène numérique. L'ingénierie pédagogique sera élaborée par les enseignants en cybersécurité de l'Académie, accompagnés d'experts. Les modules seront ensuite déployés à travers l'animation des ateliers précités. Afin de permettre l'initiation et les mises en situation concrètes, le projet mettra à disposition des équipements informatiques dédiés au sein de 3 Fab'Labs dans un premier temps, puis des 6 autres avec l'appui de la Région Guadeloupe. Une articulation sera prévue avec des événements tels que Demain spécialiste cyber, la Semaine du numérique et des sciences informatiques, Capture the flag : Passe ton Hack d'abord de la 2nde à Bac+2[10] co-organisé par le commandement de la cyberdéfense et la Direction générale de l'enseignement scolaire. En Martinique, on valorisera les actions du Safer Internet Day et la Semaine du numérique en ciblant la

[9] Voir par exemple cette vidéo.

[10] Secondes GT SNT, professionnelle Métiers des transitions numérique et énergétique ; premières/terminales G spécialité mathématiques et NSI, technologiques filières STMG et STI2D, professionnelles filière CIEL ; BTS CIEL, SIO et mentions complémentaires SNO et cybersécurité.

cybersécurité pour les écoles, collèges et lycées. Le projet conduira à concevoir un escape game pour les élèves de 3ème (1 séance de 2h pendant 3 ans), ainsi qu'un défi Capture the flag : Passe ton Hack d'abord pour les élèves de 2nde.

Sous-WP 1. 2. Sensibilisation à la cybersécurité et promotion de l'hygiène numérique à destination du grand public à travers les actions suivantes :

- Création d'une version améliorée du « Serious Game » Opération Skybreak (mis en place par l'ACCYB) qui aura la capacité d'atteindre un public plus large
- Mise en place d'un Hackathon Formation en présentiel en s'appuyant sur le Hackathon Challenge, en lien avec la cybersécurité, organisée par l'ACCYB
- Montée en puissance du programme Orange Digital Center avec des ateliers numériques d'acculturation autour de 6 thématiques : Sécurité et confiance numérique, Protection des données personnelles, Se protéger des arnaques en ligne, Protection de son identité numérique, Réseaux sociaux et esprit critique, Jeunes et cyber harcèlement. Publics visés : jeunes adultes fragiles, accessibles par les missions locales et le RSMA ; jeunes en formation d'adulte, accessibles via les CFA académiques ; publics séniors, accessibles par les associations de séniors, les CCAS et autres structures communales. Une formation d'animateurs sera mise en place pour étoffer les ressources humaines et faciliter le déploiement des ateliers, parmi les apprenants en formation d'animation sociale et socio-culturelle et de la relation client.
- Soutien au renforcement de l'utilisation du CléA numérique, une certification interprofessionnelle reconnue nationalement garantissant l'acquisition d'un socle de connaissances et de compétences commun (voir module 4, Appliquer les règles et bonnes pratiques de la sécurité numérique)

Sous-WP 1. 3. Modules d'initiation aux compétences de base en cybersécurité les publics post-bac et les étudiants de l'UA (L1 et L2) ouverts aux primo-entrants de l'UA, aux stagiaires de la formation continue et aux salariés des administrations et entreprises qui pourront donner lieu par la suite à une offre de micro-certification. Tous les primos-arrivants de l'UA seront sensibilisés via un appui sur le référentiel PIX (Sécurisation de l'environnement des pratiques numériques). Un module d'enseignement spécifique sera introduit en L2 pour les mathématiciens et informaticiens.

Nombre d'heures prévisionnelles

- Actions de sensibilisation/attraction pour les scolaires : séances de 1 à 2h selon les formats
- Modules d'initiation aux compétences de base : L1 : 10h, L2 MATHS-INFO : 24h
- Modules de formation aux compétences numériques de base et à l'hygiène numérique : 74h

Titres, certifications ou diplômes proposés : Certificat national CléA numérique ; à terme, micro-certifications cybersécurité pour les professionnels et stagiaires de la formation continue

Débouchés : Orientation des jeunes vers les formations en cybersécurité

Partenaires impliqués

- Rectorats de Guadeloupe et de Martinique (pilotes)
- ACCYB (événementiel de sensibilisation) (pilote)
- Université des Antilles (modules de sensibilisation pour les étudiants de L1/ L2)
- Orange Antilles-Guyane (mobilisation du programme Orange Digital Center)
- GRETA-CFA de la Guadeloupe (déploiement du CléA numérique)
- Organisations soutenant le projet, dont AFDAS (mobilisation et financement autour du CléA numérique)

Estimation du public touché

- Sensibilisation en collège et lycée : 720 lycéens et collégiens/an
- Sensibilisation grand public : escape game : 400 personnes/an, hackathons : 100 personnes/an, Ateliers Orange Digital Center : 1 000 personnes/an en comptant les 4 territoires
- Modules d'initiation compétences de base : plusieurs centaines d'étudiants par an (primo-entrants, L2)
- CléA numérique : 30 salariés/an

Work-package 2 : Formation initiale en cybersécurité

Objectifs
- Proposer une offre complète de formation initiale en cybersécurité afin de garantir un vivier de professionnels formés à ces compétences sur le territoire
- Proposer une offre de formation experte et certifiante en cybersécurité
- Favoriser l'insertion professionnelle, notamment à travers un dispositif de formation en alternance

Description des actions
Sous-WP 2. 1. Création d'un parcours « Cybersécurité » au sein de la Licence Informatique, accessible en alternance - public ciblé : BTS CIEL, BUT INFO, Licence 2 Informatique ou équivalent. Ce parcours enrichira l'éventail de formations déjà disponibles à l'UA, où deux autres parcours de la licence, Informatique et MIAGE, conduisent respectivement vers des Masters en Informatique et en MIAGE. Ce nouveau parcours vise un double objectif: (i) acquérir le socle fondamental de connaissances et de compétences de la cybersécurité ; (ii) préparer à une poursuite en Master sur la sécurité des systèmes d'informations. L'introduction de ce parcours ne perturbera pas les effectifs des formations existantes, car il cible principalement les étudiants issus des BTS CIEL et du BUT INFO, déjà sensibilisés à la cybersécurité et sans perspectives de poursuite d'études locales. Enfin, ce parcours aura une dimension professionnalisante forte, puisqu'il sera ouvert exclusivement en alternance avec participation de professionnels du territoire.
Sous-WP 2. 2. Création d'un parcours « Sécurité du numérique » au sein du Master MIAGE de l'UA - Public ciblé : Licence 3 Informatique - parcours Cybersécurité ou équivalent. Le Master MIAGE vise à donner une double compétence aux étudiants : en Informatique et en Gestion des entreprises. Le parcours « Sécurité du numérique » s'ajoutera au parcours existant « Science des données et Application » et aura pour objectif de former des cadres avec un haut niveau d'expertise en cybersécurité. Il sera ouvert exclusivement en alternance et facilitera les contrats d'apprentissage et de professionnalisation dans les différents territoires du projets avec des périodes d'apprentissage longues (entre 2 et 3 mois). Il inclura également la préparation à la certification ISO 27001 durant l'année de Master 2.

Nombre d'heures prévisionnelles
- Parcours Cybersécurité Lic. Informatique : 500h (dont 40 % réalisées par des professionnels du territoire)
- Parcours « Sécurité du numérique » Master MIAGE : 500h en Master 1ère année (dont 40 % réalisées par des professionnels du territoire), 400h en Master 2ème année (dont 10 % dédiées à la préparation et de la certification et 40 % réalisées par des professionnels du territoire)

Titres, certifications ou diplômes proposés : Licence Informatique parcours Cybersécurité, Master MIAGE parcours Sécurité du numérique, Préparation à la Certification ISO 27001 en Master 2

Débouchés
- Poursuite en Master et/ou en Doctorat

- Insertion professionnelle : Administrateur système/réseau/base de donnée, Responsable de la sécurité des systèmes d'information, Consultant en sécurité informatique, Architecte systèmes et logiciels, Ingénieur en Cybersécurité, Délégué à la protection des données, Chef de projet informatique

Partenaires impliqués
- **Université des Antilles (pilote)**
- **GRETA-CFA de la Guadeloupe** (mise en œuvre formations en apprentissage et professionnalisation)
- Réseau des organisations soutenant le projet (Orange, EXODATA, Gendarmerie Nationale) : accueil et recrutement des alternants

Estimation du public touché
- Parcours cybersécurité au sein de la licence informatique : 10 à 15 étudiants/an
- Parcours Sécurité du numérique au sein du Master MIAGE : 8 à 12 étudiants/an

Work-package 3 : Formation continue en cybersécurité

Objectifs
- Faciliter la montée en compétences des professionnels en cybersécurité
- Favoriser les reconversions professionnelles dans le domaine de la cybersécurité
- Proposer une offre de formation aux demandeurs d'emploi
- Mettre en place un modèle vertueux en cascade : former des profils clés au sein des organisations qui poursuivront la formation des salariés en interne

Description des actions

Sous-WP 3. 1. Accompagnement des **dirigeants et chefs d'entreprises** pour leur proposer un diagnostic action au niveau RH et organisationnel dans le domaine de la cybersécurité

Sous-WP 3. 2. Création d'un Diplôme universitaire Cybersécurité adressé à des salariés ou demandeurs d'emploi titulaires d'un BTS ou DUT en informatique (bac+2) et plus, accessible en alternance ou en formation continue pour former des professionnels capables de maîtriser, analyser, concevoir, implémenter des solutions de sécurité des systèmes et réseaux informatiques. Inclut une préparation à la certification ISO 27001.

Sous-WP 3. 3. Préparation du Titre de Technicien Supérieur Système Réseaux - option cybersécurité accessible en alternance : formation de professionnels qui maîtrisent l'installation, le maintien du fonctionnement et de l'utilisation d'infrastructures informatiques, et accompagnent les utilisateurs tant dans la prise en main qu'au niveau des dysfonctionnements. Ils interviennent également sur la sécurité des réseaux, du diagnostic à la résolution de dysfonctionnements. La polyvalence de ce professionnel en fait un véritable atout pour les petites entreprises. Cette formation pourra être complétée par le DU cybersécurité (compétences expertes).

Titres, certifications ou diplômes proposés : Diplôme universitaire Cybersécurité, Titre professionnel de Technicien Supérieur Système Réseaux - option cybersécurité, de niveau 5, préparation à la Certification ISO 27001

Nombre d'heures prévisionnelles
- Diplôme universitaire Cybersécurité : 180h
- Préparation du Titre de Technicien Supérieur Système Réseaux - option cybersécurité : 900h

Débouchés : Administrateur système/réseau/base de données, Administrateur d'infrastructures sécurisées, Technicien Supérieur Système Réseaux, Responsable de la sécurité des systèmes d'information, Consultant en sécurité informatique

Partenaires impliqués
- GRETA-CFA de Guadeloupe (pilote)
- Université des Antilles (mise en place du Diplôme Universitaire)
- ACCYB (accompagnement des entreprises)
- Organisations soutenant le projet (OPCO AFDAS, Orange Antilles-Guyane, CLUSIR, EXODATA, Gendarmerie Nationale, UDE-MEDEF, France Travail (actions également envisagées avec l'OPCO AKTO et le CNFPT) : accueil d'alternants, promotion des actions

Estimation du public touché
- Diplôme universitaire : 15 apprenants par an à partir de la rentrée 2025/2026
- Titre de Technicien Supérieur Système Réseaux - option cybersécurité : 15 apprenants /an
- Accompagnement des dirigeants : 55/an
- Certifications Iso 27001 : 30 apprenants/an

Work-package 4 : Formation de formateurs et soutien à l'insertion professionnelle

Objectifs
- Formation de formateurs garantissant la pérennité du dispositif
- Soutien à l'insertion professionnelle et rétention des talents et des compétences sur le territoire

Description des actions
Sous-WP 4. 1. Formation de formateurs (enseignants-chercheurs de l'UA, personnels des Rectorats, formateurs du GRETA-CFA) à travers la mobilisation de formateurs professionnels, conduite sur les 2 premières années du projet. Inclut une capacité à former à la préparation de la certification ISO 27001
Sous-WP 4. 2. Soutien à l'insertion professionnelle en interaction avec France Travail et avec le réseau des entreprises partenaires, notamment via la mobilisation du Conseil pédagogique et stratégique (voir section 2. 2. 2. ci-dessous), composé d'experts du territoire et de représentants du tissu économique

Nombre d'heures prévisionnelles Formation de formateurs : 30h

Partenaires impliqués
- GRETA-CFA de Guadeloupe (pilote)
- Université des Antilles, Rectorats de Guadeloupe et de Martinique (vivier de personnels formés)
- ACCYB, France Travail, autres organisations soutenant le projet (interface avec les employeurs)

Estimation du public touché Formation de formateurs : 30 personnels au total

Work-package 5 : Pilotage et communication

Objectifs
- Mettre en place un dispositif de pilotage collégial et efficace du projet
- Assurer l'amélioration continue et l'adaptation des formations à l'évolution des compétences

- Garantir un suivi appuyé sur les données à travers un recueil d'indicateurs pertinents - Garantir la pérennité du projet - Assurer la communication autour des formations ainsi que leur promotion, mettre en place une communauté de pratiques et créer une dynamique autour du projet
Description des actions **Sous-WP 5. 1. Mise en place des instances de pilotage du projet et de l'équipe-projet** (voir sections 2. 1. et 2. 2. ci-dessous) **Sous-WP 5. 2. Mise en place d'un système de suivi** appuyé par un recueil d'indicateurs pertinents (voir section 2. 2. ci-dessous) **Sous-WP 5. 3. Élaboration et déploiement d'un plan de communication autour des formations** (supports de communication diffusés auprès des publics scolaires, communication sur les réseaux sociaux et dans les médias locaux, communication auprès des entreprises) **Sous-WP 5. 4.** Organisation et participation à des **événements de promotion des formations** (Salons, Semaine de l'alternance, Forum des métiers etc.) (voir détail en section 1. 4.) **Sous-WP 5. 5. Animation d'une communauté de pratiques** autour des formations
Partenaires impliqués **- Université des Antilles (pilotage) et ACCYB (communication et communauté de pratiques)** - Ensemble des partenaires du projet (gouvernance du projet et actions de communication) - Organisations soutenant le projet : communication et promotion des actions

■ 1. 2. 3. Les modalités pédagogiques et d'accompagnement

Les formations du dispositif CyberEDAntilles seront proposées **sur les territoires de Guadeloupe, Martinique**, et ouvertes au public de **Saint-Martin et Saint-Barthélemy**. Dans le cas des formations initiales de licence et de Master (WP2), les cours magistraux seront conduits en **modalité hybride**, et les TD seront dédoublés (conduits en présentiel sur chacun des deux pôles de l'UA). Dans ses différents domaines d'implémentation, CyberEDAntilles mobilisera des **formats pédagogiques innovants et attractifs** qui incluront une **formation par la pratique, réalisée notamment en articulation :**

- **avec les Rectorats de Guadeloupe et de Martinique** pour une sensibilisation au collège et au lycée appuyée sur des pratiques ludiques sur le modèle du dispositif Cyberenjeux proposé par l'ANSSI et à travers l'utilisation de fablabs dédiés ;
- en articulation avec le projet d'**Institut du numérique** en cours de consolidation par la **Collectivité territoriale de Martinique** et avec le projet de **Laboratoire cyber** de **l'ACCYB** mis en place en Guadeloupe, un lieu de type Fablab permettant de réaliser des tests en matière de sécurité (p. ex. : tests sur des virus nécessitant des espaces fermés/sécurisés).

De plus, CyberEDAntilles s'appuie sur le dispositif de la **formation en alternance,** qui permettra de renforcer le lien avec le monde socio-économique et l'insertion professionnelle des apprenants. CyberEDAntilles mobilisera également des techniques de **réalité virtuelle**, sur la base d'une première expérimentation pilote conduite par des enseignants-chercheurs de l'UA qui a démontré la valeur ajoutée de l'apprentissage par réalité virtuelle, notamment au sein des enseignements en informatique[11]. Nous procéderons à l'équipement de 2 **salles de TD pour enseignements**

[11] Pluton, L. et Stattner, E. (2023). Influence de l'envir ne nt de formation à distance sur l'engagement des apprenants et apprenantes : une expérimentation autour de la réalité virtuelle.

hybrides/technologies Hyflex sur les Pôle de Guadeloupe et de Martinique de l'Université.
CyberEDAntilles a pour particularité de préparer les futurs professionnels antillais aux **spécificités de ce secteur sur leur Bassin géographique**. En plus du socle de compétences fondamentales et techniques, il proposera des **modules complémentaires et pluridisciplinaires liés aux aspects juridiques, géopolitiques ou économiques propres au Bassin caribéen** : origine des attaques, gestion de crise en écosystème insulaire, spécificités juridiques locales, infrastructures.
Les formations mises en place seront labellisées à travers le LABEL SECNUMEDU (formations longues) et le LABEL SECNUMEDU formation continue. Des intervenants seront mobilisés à travers les **réseaux d'experts** des partenaires, notamment l'ACCYB. Lorsque des prestataires externes seront mobilisés, ceux-ci seront sélectionnés sur la base de critères de qualité (certification Qualiopi), et dans le respect des règles de la commande publique.

■ 1. 2. 4. Les mesures en faveur de la transition sociétale

CyberEDAntilles est pensé dans une démarche d'inclusivité, aussi bien du point de vue des publics visés que des intervenants au sein des formations. Cela se traduira notamment par :

- un **ciblage des publics éloignés** (public féminin, publics fragiles, dans les **actions de sensibilisation/attraction vers la filière** ;
- un **ciblage des publics vulnérables** (publics séniors, recours à la langue créole dans les formations) dans les actions de sensibilisation à l'hygiène numérique ;
- une cible d'**un tiers de femmes** minimum pour les actions de **formation de formateurs**, de façon à garantir ce même ratio au sein du vivier de formateurs du dispositif.

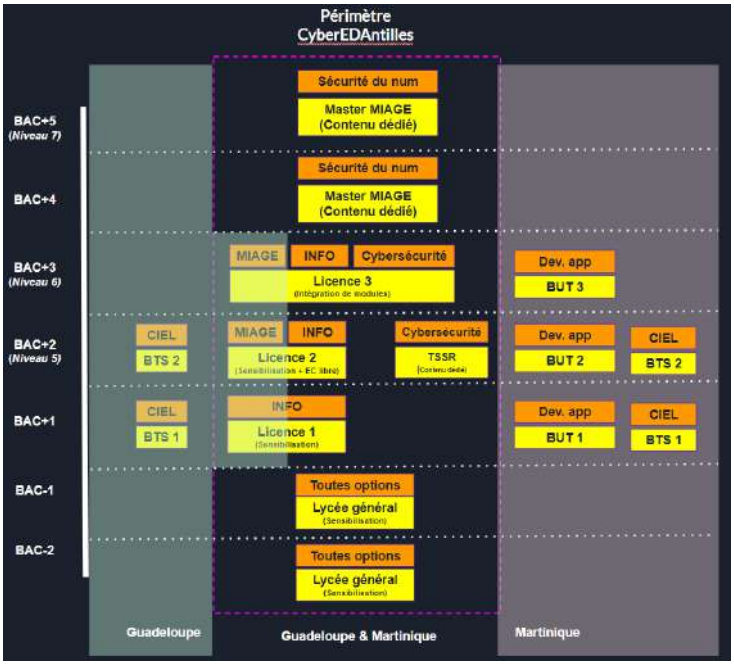
Cette politique d'inclusivité est notamment au centre de la stratégie du programme **Orange Digital Center**, partenaire du projet dont l'une des priorités est de s'adresser à des publics éloignés ou fragiles (Quartiers politiques de la ville, mobilisation d'experts de l'inclusion des séniors, prise en compte de l'illectronisme, accompagnement à l'entrepreneuriat féminin digital).
En termes de **transition environnementale**, un défi propre au projet tient à la multi-insularité de son champ de déploiement (Guadeloupe, Martinique, St-Martin, St-Barthélemy). Les mesures de **pédagogie hybride** mentionnées plus haut auront notamment pour fonction de **limiter l'impact environnemental** du projet en évitant les déplacements des formateurs ou des apprenants. Par ailleurs, le fait de procéder à des actions de **formation de formateurs**, puis de former un **vivier de compétences locales** en cybersécurité permettra d'internaliser ces compétences et d'éviter de mobiliser des experts en provenance de l'Hexagone.

○ 1. 3. RESULTATS ET MESURE DE L'IMPACT

Sur la base des effectifs moyens par action proposés dans la description des work-packages ci-dessus, nous estimons que le dispositif CyberEDAntilles permettra de former et sensibiliser directement **4 200 personnes**[12] au total au bout des 5 ans de la période de financement, en tenant compte de l'amorçage puis de la montée en puissance. Au-delà de cette période (en rythme de croisière une fois le dispositif parvenu à maturité), il est attendu que près de **950 personnes par an** soient directement formées et/ou sensibilisées. En plus de cela, des centaines de personnes sur les 4 territoires de déploiement du projet seront touchées par les actions de sensibilisation destinées au grand public (Escape game, hackathon, Orange Digital Center, événementiel etc.).
En termes de **risques**, le principal risque identifié tient à la capacité à **dégager un vivier suffisant de participants aux formations**, notamment sur un ensemble de territoires insulaires. Ce risque est néanmoins jugé comme contrôlé à travers une analyse des flux de publics-cibles au sein du

[12] Nous avons révisé l'estimation du public touché par le dispositif CyberEDAntilles par rapport à la lettre d'intention en faisant une distinction plus claire entre les personnes directement formées/sensibilisées et les actions de sensibilisation destinées au grand public.

projet, que nous représentons par le graphique ci-dessous. Il est ainsi attendu que les BTS CIEL alimentent majoritairement le parcours Cybersécurité de la Licence Informatique. Des actions de sensibilisation spécifiques seront de plus prévues aux différents niveaux de formation définissant le périmètre du projet, pour renforcer l'attraction vers les formations proposées dans le projet.



○ 1. 4. DIFFUSION DES DISPOSITIFS ET DES RESULTATS

L'élaboration et le déploiement d'un **plan de communication** autour des formations seront assurés au sein du Sous-WP 5. 3. Cela impliquera des activités de **promotion des formations proposées** sur les sites internets des partenaires, sur les plateformes nationales (notamment Mon Master) et sur le site web du GRETA-CFA de la Guadeloupe et des partenaires. Les actions de sensibilisation à destination des différents publics scolaires, professionnels et généralistes prévues au WP1 permettront également une diffusion de l'information autour de ces formations, notamment à travers des supports dédiés (brochures, flyers). Les partenaires du projet seront présents sur les **événements locaux d'orientation présentiels et en ligne**, notamment les Journées portes ouvertes de l'Université, le Salon de l'Orientation, de la Formation et des Métiers de Guadeloupe, le Salon virtuel de l'orientation de Guadeloupe, la Semaine de l'alternance, le Salon Formeo en Martinique ou encore le Forum des métiers à Saint-Barthélemy. Une démarche de **dissémination des résultats** sera conduite dans une volonté d'essaimage. Les études d'impact conduites sur le projet seront publiées aussi bien sur des canaux de communication grand public (sites internets des partenaires) qu'à travers des publications en sciences de l'éducation dans la lignée de la publication indiquée plus haut sur l'impact des pédagogies basées sur la réalité virtuelle. L'ACCYB pilotera l'animation d'une communauté de pratiques, et mobilisera le réseau en cours de mise en place au sein du Bassin Caraïbe (îles néerlandaises, Trinidad, Jamaïque).

● 2. ORGANISATION ET PILOTAGE DU PROJET

○ 2. 1. ORGANISATION DU CONSORTIUM

Le **modèle du pilotage du projet** aura 2 objectifs complémentaires : assurer le **suivi de la feuille de route du projet** pendant la période de financement et, de façon pérenne, garantir **la pertinence et l'actualisation des formations proposées**. Afin de répondre à ces deux objectifs, la gouvernance et le pilotage du projet seront proposés de la façon suivante :

Le **Comité de pilotage** sera **présidé par l'Université des Antilles** en tant que chef de file, et comprendra **un représentant de chaque partenaire** (ACCYB, GRETA-CFA de Guadeloupe, Rectorats de Guadeloupe et de Martinique, Orange Antilles-Guyane). Il définira la vision, la mission et les objectifs à long terme du projet et supervisera la mise en œuvre des activités. En plus de l'objectif direct qui est de créer conjointement une offre de formation d'excellence sur la cybersécurité aux Antilles, la mise en place de ce Comité de pilotage aura pour valeur ajoutée fondamentale de contribuer à la **structuration de l'écosystème public/privé autour de la cybersécurité sur ces territoires**. Il se réunira 1 fois par mois dans la première année du lancement projet, puis une fois tous les 3 mois une fois le dispositif pleinement installé.

○ 2. 2. PILOTAGE DU PROJET

■ 2. 2. 2. Dispositif de pilotage

Le Comité de pilotage sera secondé par une **équipe opérationnelle** qui comprendra le coordinateur et le responsable de qualité et communication qui seront recrutés spécifiquement, ainsi que les coordinateurs des work-packages. Cette équipe se réunira tous les mois.

De plus, le dispositif comprendra un **Conseil pédagogique et stratégique** réunissant des experts et parties prenantes désignés par le Comité de pilotage (p. ex. experts en cybersécurité, représentants des employeurs ou des filières, collectivités territoriales, membres de l'ANSSI). Ce Conseil instruira la démarche d'amélioration continue en assurant une veille sur les besoins en compétences sur l'évolution du secteur. Il réalisera une **étude de mi-parcours** sur l'évolution de la carte des formations en cybersécurité en lien avec le marché de l'emploi, ainsi qu'un **bilan final avec analyse d'impact.** Le projet sera mesuré au moyen d'un système d'indicateurs couvrant les aspects suivants[13] :

- **Sensibilisation** : %age de collèges et de lycées du territoire touchés par an, distribution sur les 4 îles du périmètre du projet, nb d'élèves touchés, nb de professionnels participant aux formations aux compétences de base, nb d'événements grand public organisés par an
- **Attractivité des parcours** : accroissement du nb de personnes attirées vers la filière à terme, accroissement du %age du public féminin au sein des formations
- **Formation** : nb de personnes formées par an en licence, nb de personnes formées par an en Master, nb d'inscrits au DU en cybersécurité par an, nb de certifications obtenues par an
- **Impact socio-économique** : tx d'insertion professionnelle, nb de reconversions professionnelles, nb de salariés accompagnés, nb d'emplois créés, nb d'entreprises créées offrant des services de cybersécurité, diminution du nb de cyberattaques, réduction du temps

[13] L'affinage du système d'indicateurs et la définition de cibles correspondante seront inclus dans la fiche de poste du responsable qualité recruté pour le projet

de gestion des incidents liés aux cyberattaques

- **Inclusivité du dispositif** : %age de public féminin parmi le public formé, %age de public féminin au sein de la formation de formateurs, %age de public touché au sein des territoires éloignés, nb de séniors touchés par le projet
- **Soutenabilité du dispositif** : revenus générés par le projet

■ 2. 2. 3. Calendrier de mise en œuvre

Année	Année 1				Année 2				Année 3				Année 4				Année 5			
Trimestre	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Work-package 1 : Sensibilisation et attraction vers la filière																				
Sous-WP 1.1. Déploiement d'équipements dans les trois Fab'Labs																				
Sous-WP 1.1. Mise en place d'ateliers de sensibilisation dans les Fab'Labs																				
Sous-WP 1.2. Ateliers Orange Digital Center																				
Sous-WP 1.2. Lancement du Serious Game Cyber																				
Sous-WP 1.2. Organisation d'un Hackathon Formation en cybersécurité																				
Sous-WP 1.3. Mise en place des modules de sensibilisation																				
Work-package 2 : Formation initiale en cybersécurité																				
Ingénierie pédagogique et élaboration des maquettes																				
Equipement des salles pour l'enseignement en hybride																				
Sous-WP 2.1. Lancement du parcours Cybersécurité de la licence Informatique																				
Sous-WP 2.2. Lancement du parcours Sécurité du numérique du M1 MIAGE																				
Sous-WP 2.2. Lancement du parcours Sécurité du numérique du M2 MIAGE																				
Work-package 3 : Formation continue en cybersécurité																				
Ingénierie pédagogique et élaboration des maquettes																				
Sous-WP 3. 1. Accompagnement des dirigeants et chefs d'entreprises																				
Sous-WP 3. 2. Création d'un Diplôme universitaire Cybersécurité																				
Sous-WP 3. 3. Préparation du Titre de Technicien Supérieur Système Réseaux																				
Work-package 4 : Formation de formateurs et soutien à l'insertion pro.																				
Sous-WP 4. 1. Formation des formateurs																				
Work-package 5 : Pilotage et communication																				
Sous-WP 5. 1. Mise en place des instances de pilotage et de l'équipe-projet																				
Sous-WP 5. 2. Suivi du projet et evaluation du dispositif																				
Sous-WP 5. 2. Etude de mi-parcours sur l'évolution de la carte des formations																				
Sous-WP 5. 3/4/5. Communication et promotion de la nouvelle offre de formation																				
Premiers retours d'expérience et adaptation du dispositif																				

○ 2. 3. PERENNITE DES DISPOSITIFS MIS EN PLACE

Les formations mises en place au sein du projet sont conçues de façon pérenne, et le financement demandé s'inscrit dans une démarche de **fonds d'amorçage**. Une partie des financements correspond à un **investissement initial** qui n'aura **pas besoin d'être réitéré** (ingénierie pédagogique, équipements, formation de formateurs). En plus de cela, le projet permettra de dégager progressivement des ressources, notamment à travers les **droits d'inscription** (DU) ou le renforcement des relations avec les entreprises. La labellisation CMA facilitera également l'attraction de ressources complémentaires (p. ex. Interreg, mécénat). Enfin, l'inscription dans le projet d'une **formation de formateurs** sert directement l'objectif de pérennisation du dispositif, en mettant en place un modèle vertueux en cascade pour le transfert de compétences.

En termes de **gouvernance**, le pilotage en mode projet cédera la place au terme de la période de financement à une gouvernance en continu visant à garantir en particulier la bonne évolution de la carte des formations. Le modèle définitif sera mis en place par le Comité de pilotage pendant la deuxième phase du projet, et les partenaires s'engagent à dédier les ressources requises pour ce modèle d'atterrissage.

● 3. JUSTIFICATION DES DEPENSES DU PROJET

CyberEDAntilles comporte un **coût total de 5 079 322 €** (hors frais d'environnement), dont **2 940 276 € (57,89 %)** sont demandés au titre de la subvention[14]. L'apport des partenaires s'élève à **2 139**

[14] Le budget a été revu à la baisse par rapport au montant indiqué dans la lettre d'intention pour tenir compte des remarques proposées par les évaluateurs.

046 €, répartis de la façon suivante (hors frais d'environnement) : UA - 609 272 € ; ACCYB - 256 360 €, GRETA-CFA Guadeloupe - 911 176 € ; Rectorat de Guadeloupe - 162 165 €, Rectorat de Martinique - 100 563 €, Orange Antilles-Guyane - 99 510 €. Le montant des **co-financements privés** (ACCYB et Orange Antilles-Guyane) est de **355 870** €. De plus, la **Collectivité territoriale de Martinique** et l'UA ont signé une Convention d'objectifs et de moyens 2023 - 2026, dont l'un des axes porte sur la construction d'une offre de formation avec co-financement à hauteur de 1,6M €. L'UA envisage de mobiliser une partie de ce financement à hauteur de **300 000 €** sur la période du projet qui viendront s'ajouter aux co-financements indiqués dans l'annexe financière.

Le budget du projet a été élaboré par un **calcul des coûts année par année**, avec un **modèle « en cloche »** : montée en puissance progressive (année 1 et 2), puis stabilisation et dégressivité en années 4 et 5 pour préparer l'absorption des coûts. Il intègre une **problématique de surcoûts** propres aux territoires ultramarins et au territoire antillais en particulier : projet qui couvre 2 régions académiques et 4 collectivités territoriales sur 2 835 km^2, ce qui engendre des **frais de déplacement** et d'équipement pour les modalités hybrides ; coûts liés à l'**importation des équipements** et à la **mobilisation de formateurs de l'Hexagone pour la formation de formateurs** ; surcoût de la **masse salariale** (indexation des salaires de 40%).

N°	Titre de l'action/de l'axe	Principaux postes de dépenses	Budget prévu (k€[15])	Aide demandée (k€)
1	WP1 sensibilisation et attraction vers la filière	Ingénierie pédagogique, indemnités intervenants experts et vacations, missions, supports de communication, encadrement administratif et pédagogique, équipements, fonctionnement événementiel	1142k€	610k€
2	WP2 Formation initiale	Ingénierie pédagogique, enseignements (vacation, enseignants contractuels, enseignements externalisés), encadrement administratif et pédagogique, équipements et maintenance (dont réalité augmentée, hybridation, laboratoire cyber), prestations de certification	2150k€	1203k€
3	WP3 Formation continue	Ingénierie pédagogique, enseignements (vacations, enseignants contractuels, enseignements externalisés via des prestataires), encadrement administratif et pédagogique, prestations de certification, équipements et matériel informatique	370k€	24k€
4	WP4 Formation de formateurs et insertion professionnelle	Formations de formateurs (prestations externalisées), budget de fonctionnement communication, missions	153k€	96k €

[15] Hors frais d'environnement et hors frais généraux.

5	WP5 Pilotage et communication	Recrutement coordinateur projet et responsable qualité et communication, participation partenaires aux instances du projet (coût RH et missions), budget de fonctionnement communication et participation à de l'événementiel sur les différentes îles (salons…), prestations intellectuelles pour le suivi de la cartographie formations	816k€	564k €

Fiche partenaire n°4 : Identification et budget

N° de partenaire	2023-04
Acronyme	CyberEDAntilles

Identification de l'établissement partenaire

Nom complet du partenaire	Agence Caribéenne pour la Cybersécurité
Sigle du partenaire	ACCYB
Forme juridique	Petite entreprise
N° de SIRET	Saisir un n°SIRET de 14digits 918 714 890 00012
Assujetti à la TVA	

Personne habilitée à représenter juridiquement l'établissement partenaire (pour signature du contrat attributif d'aide ou de reversement)

Genre	Mme
Prénom	Marie-Lucienne
Nom	RATTIER
Qualité	PRÉSIDENTE

Demande financière détaillée du projet (montant HT en €, incluant la TVA non récupérable le cas échéant)

Equipements ou amortissement d'équipements de R&D

Seuil d'immobilisation propre à l'établissement	800 €	Le coût d'achat est égal ou supérieur au seuil d'immobilisation.

			Descriptif	WP concerné	Sous-WP	Coût d'achat (en €)	Pourcentage d'utilisation (en %)	Coût total (en €)	Assiette de l'aide (en €)
1			Escape game 2D	WP 1	.2	60 000 €	50,0 %	30 000 €	0 €
2			Monter en puissance de l'escape game existant (e.g. une version en 3D et différents	WP 1	.2	120 000 €	100,0 %	120 000 €	120 000 €
3			Laboratoire Cyber (Sonde de sécurité, Data lake, environnement de test) - Création d'une	WP 2	.2	300 000 €	40,0 %	120 000 €	113 000 €
			Total					270 000 €	233 000 €

Personnels sans financement

		Catégorie de personnel	Descriptif	WP concerné	Sous-WP	Coût mensuel (en €)	Personne. Mois	Coût total (en €)	
1		Autre	Préparation et animation Hackathon "challenge" Cybersecurité avec public cible	WP 1	.2	8 000 €	3,1	24 800 €	
2		Autre	Préparation et animation du Hackathon "Formation" Cybersecurité: passer du format	WP 1	.2	8 000 €	3,1	24 800 €	
3		Autre	Formation des aidants "Diagnostic Cyber" pour l'accompagnement des dirigeants dans	WP 3	.1	8 400 €	3,4	28 560 €	
4		Autre	Participation au COPIL et coordination du WP 1	WP 5	.1	8 000 €	5,4	43 200 €	
			Total				15,0	121 360 €	

Personnels avec financement en contrat à durée déterminée

		Catégorie de personnel	Descriptif	WP concerné	Sous-WP	Coût mensuel (en €)	Personne. Mois	Coût total (en €)	Assiette de l'aide (en €)
1									
2									
3									
			Total				-	- €	- €

Personnels avec financement en contrat à durée indéterminée

		Catégorie de personnel	Descriptif	WP concerné	Sous-WP	Coût mensuel (en €)	Personne. Mois	Coût total (en €)	Assiette de l'aide (en €)
1									
2									
3									
			Total				-	- €	- €

Heures complémentaires d'enseignement et modulation de service (établissements d'enseignement et formation, organismes de recherche)

			Descriptif	WP concerné	Sous-WP			Coût total (en €)	Assiette de l'aide (en €)
1									
2									
3									
			Total					- €	- €

Reconnaissance au titre des activités prévues au référentiel horaire (établissements d'enseignement et formation, organismes de recherche)

			Descriptif	WP concerné	Sous-WP			Coût total (en €)	Assiette de l'aide (en €)
1									
2									
3									
			Total					- €	- €

Prestations de service externes

			Descriptif	WP concerné	Sous-WP			Coût total (en €)	Assiette de l'aide (en €)
1									
2									
3									
			Total					- €	- €

Missions

			Descriptif	WP concerné	Sous-WP			Coût total (en €)	Assiette de l'aide (en €)
1			Missions pour 2 encadrants par territoire (Guadeloupe, Martinique et Saint-Martin) pour	WP 1	.2			75 000 €	0 €
2			Mission pour intervenants du Hackathon "Formation" Cybersecurité: passer du format	WP 1	.2			50 000 €	50 000 €
3									
			Total					125 000 €	50 000 €

Fiche partenaire n°4 : Identification et budget

N° de partenaire	**2023-04**
Acronyme	**CyberEDAntilles**

Autres dépenses externes (consommables, petits matériels ...)

			Descriptif	WP concerné	Sous-WP			Coût total (en €)	Assiette de l'aide (en €)
1									
2									
3									
Total								- €	- €

	Taux (en %)		Coût total (en €)	Assiette de l'aide (en €)
Frais généraux (max. 20% des coûts entrant dans l'assiette de l'aide)	20,0 %		56 600 €	56 600 €
Taux d'environnement (compris entre 0 et 100 % ; uniquement pour les organismes publics)			0 €	
Coût complet du projet (hors frais d'environnement, en €)	**572 960 €**			
Total éligible pour le calcul de l'aide : Total assiette de l'aide (en €)			**339 600 €**	
Taux d'aide demandé (%)	**Taux max 60%**		**60,0 %**	
Aide demandée (en €)			**203 760 €**	
Coût complet du projet comprenant les frais d'environnement (en €)	**572 960 €**			

Autres soutiens financiers (sollicités ou obtenus par le partenaire pour le projet)

Identification des financeurs	Nature et objet du financement et, le cas échéant, WP(s) et tâche(s) concernés	Type de financement (public/privé)	Montant sollicité	Montant obtenu	Date effective ou prévue du financement
		Sous-total autres financements publics	0 €	0 €	
		Sous-total autres financements privés	0 €	0 €	
		Total	- €	- €	

Publication d'informations relatives au projet

Si le projet est retenu pour financement, l'opérateur se réserve la possibilité de rendre publiques les informations suivantes : nom du responsable du projet, dénominations des partenaires qu'ils soient des entreprises ou qu'ils appartiennent à un organisme de recherche. L'opérateur ne rendra pas publiques les informations sur les personnes ou les partenaires qui en auront fait le demande.

En cas de refus de publication remplacer ci-dessous la mention "Oui" par "Non" :

Dénomination du partenaire (si "Non", celle-ci sera remplacée par la mention générique "Entreprise" ou "Organisme de recherche") : Oui

Nota : en déposant un projet, les partenaires ont accepté que l'opérateur publie l'acronyme, le titre, le résumé, l'aide accordée au projet, la date de début de projet et la durée.

Commentaires (le cas échéant)

Les informations personnelles transmises dans ces documents sont obligatoires et seront conservées en fichiers par l'opérateur pour assurer la conduite opérationnelle de l'évaluation et l'administration des dossiers.
Conformément à la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux Fichiers et aux Libertés, les personnes concernées disposent d'un droit d'accès et de rectification des données personnelles les concernant. Les personnes concernées peuvent exercer ce droit en s'adressant à l'opérateur (voir coordonnées dans le texte de l'appel à projets).

Lettre d'engagement

Le present engagement est a completer, signer, viser par la personne habilitée à engager l'Etablissement.

LIEN DU SITE DE DEPOT

https://france2030.agencerecherche.fr/CMA/accueil.php?

Ayant le pouvoir d'engager juridiquement l'établissement ci-dessus, je déclare :

• avoir pris connaissance du dossier complet de dépôt (document de description du projet, y compris son annexe, et document administratif et financier) tel que déposé sur le site de l'ANR et du règlement relatif aux modalités d'attribution des aides au titre de l'AMI- CMA ;

Fiche partenaire n°4 : Identification et budget

N° de partenaire	**2023-04**
Acronyme	**CyberEDAntilles**

▪ m'engager à négocier et signer un accord de consortium (ou équivalent) et mettre en œuvre tous les moyens nécessaires pour finaliser ce document dans les conditions et délais prévus par le règlement relatif aux modalités d'attribution des aides précité ;

▪ m'engager à mettre en œuvre tous les moyens nécessaires à la réalisation du projet tels que décrits dans le dossier de dépôt, dans les conditions prévues par le règlement relatif aux modalités d'attribution des aides précité ;

▪ m'engager à respecter les engagements financiers tels que détaillés dans le document administratif et financier du document déposé ;

▪ m'engager à mettre en œuvre les recrutements sur contrat des personnels nécessaires à la réalisation de la proposition déposée et cela en conformité avec tous les lois et règlements en vigueur applicables ; à mettre à disposition des personnels engagés dans la réalisation du projet les surfaces de travail nécessaires à l'accomplissement de leurs missions pendant la durée du projet ;

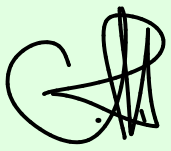
▪ souscrire aux obligations qui découlent du financement du projet par l'ANR, notamment à des fins d'évaluation globale de l'action ;

▪ que le projet ne cause pas un préjudice important du point de vue de l'environnement (application du principe DNSH – Do No Significant Harm ou « absence de préjudice important ») au sens de l'article 17 du règlement européen sur la taxonomie ;

▪ m'engager à ne pas avoir initié de travaux liés au projet déposé.

Personne habilitée à engager l'établissement partenaire (EP)

Prénom	Nom
Marie-Lucienne	RATTIER
Qualité	
PRÉSIDENTE	

Signature & Cachet


CMA

2024

Acronyme du projet

CyberEDAntilles

ANNEXE 3

RESPONSABLE DE PROJET
ETABLISSEMENTS PARTENAIRES

Nom du Responsable de projet : Erick STATTNER

Partenaires publics

Identifiant Partenaire	Nom de l'établissement partenaire
1	**Université des Antilles**
2	Collège Raizet - Groupement d'Etablissements de la Guadeloupe
3	Rectorat de la Région Académique de la Guadeloupe
6	Rectorat de l'Académie de Martinique

Partenaires privés

Identifiant Partenaire	Nom de l'établissement partenaire
4	Agence Caribéenne pour la Cybersécurité
5	Orange Antilles Guyane

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anr agence nationale de la recherche

FRANCE 2030

Action : Compétences et métiers d'avenir
Acronyme du Projet : CyberEDAntilles
Durée du Projet : 60 mois (du 01/01/2025 au 31/12/2029)
Montant total de l'aide : 2 900 000 €

CONTRAT ATTRIBUTIF D'AIDE
n° ANR-24-CMAS-0014

ENTRE

L'Agence Nationale de la Recherche (ci-après dénommée l'« ANR »), sise au 86-88 rue Regnault à Paris (75013), représentée par sa Présidente-Directrice générale, dûment habilitée à l'effet des présentes ;

d'une part,

ET

L'Université des Antilles (ci-après dénommée « le Chef de file »), sise au Campus Fouillole, à Pointe à Pitre (97110), référencée sous le numéro SIRET 199 715 855 00011 et représentée par son Président, Monsieur Michel GEOFFROY, dûment habilité à l'effet des présentes ;

d'autre part,

Ci-après dénommés ensemble les « Parties ».

VISA :

Vu le décret n° 2006-963 du 1er août 2006 modifié portant organisation et fonctionnement de l'Agence Nationale de la Recherche ;

Vu la loi de finances rectificative n°2010-237 du 9 mars 2010 de finances rectificatives pour 2010, notamment son article 8 ;

Vu la convention du 8 avril 2021 modifiée entre l'État, l'ADEME, l'Agence nationale de la recherche, la Caisse des dépôts et consignations, l'EPIC Bpifrance et la société anonyme Bpifrance encadrant les dispositions communes aux conventions relatives à la mise en œuvre du quatrième programme d'investissements d'avenir et du plan France 2030 ;

Vu la convention du 4 juin 2021 entre l'État, l'ADEME, l'Agence nationale de la recherche, la Caisse des dépôts et consignations, l'EPIC Bpifrance et la société anonyme Bpifrance relative au programme d'investissements d'avenir (action « Soutien au déploiement ») ;

Vu l'arrêté du 11 mai 2023 relatif à l'approbation du cahier des charges de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » ;

Vu le règlement financier relatif aux modalités d'attribution des aides au titre de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » ;

Vu la décision n° 2024-DEPL-062431 du Premier Ministre, en date du 3 juillet 2024, autorisant l'ANR à contractualiser avec le Chef de file sur le financement du Projet « **CyberEDAntilles** » dans le cadre de l'action « Compétences et métiers d'avenir ».

Il EST CONVENU CE QUI SUIT :

Article 1 : DÉFINITIONS

Responsable de Projet : personne physique qui assure la coordination du projet pour le compte du Chef de file.

Chef de file : Établissement porteur, doté de la personnalité morale, il est l'interlocuteur privilégié de l'Opérateur pour les aspects administratifs et financiers. Il est responsable de la mise en place et de la formalisation de la collaboration entre les Établissements partenaires, de la production des livrables du projet, de la tenue des réunions d'avancement et de la communication des résultats. Il s'appuie pour cela sur le Responsable du projet.

Établissement partenaire : c'est un des organismes de formation ou d'accompagnement, des employeurs ou leurs représentants, des collectivités territoriales, parties prenantes au projet. Chacun des Établissements partenaires désigne en son sein un correspondant du Responsable du projet.

Établissement gestionnaire : établissement partenaire du projet différent du Chef de file choisi, le cas échéant, conformément aux délégations de gestion en vigueur existant entre les Établissements publics partenaires impliqués dans le projet. L'Établissement gestionnaire de l'aide est doté de la personnalité morale.

Reversement : un Établissement partenaire peut bénéficier, en vertu d'une convention de Reversement, d'une quote-part de l'aide pour la réalisation d'une tâche ou d'une mission dans le cadre du projet, dans le respect de l'encadrement européen des aides.

Consortium ou groupement : Le groupement est composé de partenaires souhaitant répondre conjointement à l'appel à manifestation d'intérêt afin d'apporter une réponse commune aux enjeux identifiés. Ce sont des partenaires opérationnels du projet qui mettent en œuvre des moyens qui leur sont propres. Le groupement est représenté par un chef de file (le porteur de projet) auquel les autres membres du groupement donnent expressément mandat pour les représenter dans le cadre du projet. Les membres du groupement concluent un accord prévoyant, notamment, la gouvernance du projet, ses objectifs et les moyens mis en œuvre. Lorsque la subvention est attribuée à plusieurs membres, le groupement devient alors un consortium et l'accord devra également préciser la clé de répartition de la subvention et ses modalités de versement aux différents membres.

Il est alors impératif de désigner une personne morale juridiquement porteuse du projet (chef de file) capable de mettre en place une gouvernance robuste, un comité de pilotage et de suivi du projet sur toute sa durée et une animation adéquate du consortium et des parties prenantes.

Encadrement européen : l'aide versée est susceptible de constituer une aide d'Etat au sens de l'article 107, §1 du TFUE si elle soutient des activités économiques entendu comme toute offre de biens ou des services sur un marché donné. Les bases juridiques mobilisables sont : l'Encadrement des Aides d'Etat à la recherche, au développement et à l'innovation n°2022/C 414/01 du 28 octobre 2022 ou toute communication ultérieure venant s'y substituer, le régime cadre exempté n° SA. 111723 d'aides à la recherche, au développement et à l'innovation pris sur la base du règlement général d'exemption par catégorie n° 651/2014 adopté par la Commission européenne le 17 juin 2014 et publié au JOUE le 26 juin 2014, tel que modifié par les Règlements (UE) 2017/1084 de la Commission du 14 juin 2017, publié au Journal Officiel de l'Union Européenne du 20 juin 2017, 2020/972 du 2 juillet 2020 publié au JOUE du 7 juillet 2020 et 2023/1315 du 23 juin 2023 publié au JOUE du 30 juin 2023 ou tout autre régime cadre exempté validé par la Commission européenne, le règlement n° 2023/2831 de la Commission du 13 décembre 2023 « relatif à l'application des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne aux aides de minimis de minimis » et la décision de la Commission du 20 décembre 2011 « relative à l'application de l'article 106, paragraphe 2, du traité sur le fonctionnement de l'Union européenne aux aides d'État sous forme de compensations de service public octroyées à certaines entreprises chargées de la gestion de services d'intérêt économique général ».

Entreprise : au sens de la règlementation européenne sur les aides d'Etat, « *est considérée comme entreprise toute entité, indépendamment de sa forme juridique, exerçant une activité économique* ». Selon leur taille et leur importance économique, ces entités sont classées selon les trois catégories suivantes : les grandes entreprises, les petites et moyennes entreprises (PME). La définition des petites et moyennes entreprises (PME) est celle de l'Annexe 1 du Règlement (CE) n° 651/2014 de la Commission Européenne du 17 juin 2014 et figure dans la recommandation 2003/ 361/CE de la Commission Européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises et tout texte communautaire venant s'y substituer.

Article 2 : OBJET DU CONTRAT

Le Contrat a pour objet de définir les modalités de financement et d'exécution du Projet « **CyberEDAntilles** » sélectionné dans le cadre de l'action « Compétences et métiers d'avenir ».

Le Contrat comprend les annexes suivantes :

- Annexe 1 : Descriptif du Projet
- Annexe 2 : Document administratif et financier et lettres d'engagement des Établissements partenaires
- Annexe 3 : Liste des Établissements partenaires et identité du Responsable de Projet

Le Chef de file s'engage à affecter l'aide obtenue à la réalisation exclusive du Projet, conformément à l'Annexe 2 du Contrat, sous réserve des stipulations de l'article 6.1 du Règlement Financier.

Le Chef de file s'engage à réaliser avec la participation des autres Établissements partenaires dans les délais définis à l'Article 4 du Contrat, le Projet dont la description constitue les Annexes 1 et 2 du Contrat.

Les Annexes 1 à 3 susmentionnées font partie intégrante du Contrat. En cas de contradiction entre les Annexes et le Contrat, les stipulations du Contrat priment.

Article 3 : MONTANT ET GESTION DE L'AIDE

L'ANR accorde au Chef de file, au nom et pour le compte de l'État, compte tenu du montant du coût total prévisionnel du Projet indiqué en Annexe 2, une aide de **2 900 000 €**.

Le Chef de file peut transférer une partie de l'aide aux Établissements partenaires au moyen de Contrats de Reversement établies entre lui-même et chaque Établissement partenaire concerné bénéficiaire, conformément à l'Annexe 2 du Contrat et selon des modalités qu'il définit, dans le respect des droits et obligations prévus par le Contrat. A défaut, le Reversement peut s'effectuer au moyen de toute stipulation contenue dans un contrat n'ayant pas pour objet exclusif ledit Reversement de l'aide. Une copie des contrats de Reversement et de leurs éventuels avenants sera transmise à l'ANR dans un délai maximal de 60 jours calendaires à compter de leur date de signature par l'ensemble des parties.

En cas de délégation de gestion de l'aide à un Établissement gestionnaire, partenaire du projet, une copie de la convention de délégation de gestion est transmise à l'ANR dans les meilleurs délais. Il en va de même de ses éventuels avenants.

Article 4 : DURÉE DU PROJET

La date de démarrage du Projet et de prise en compte des dépenses est fixée au 01/01/2025.

La durée de réalisation du Projet est fixée à **60** mois, soit un achèvement prévu à la date du 31/12/2029 qui correspond à celle de fin de prise en compte des dépenses.

L'ANR doit être informée de l'achèvement du Projet si celui-ci intervient avant la date prévue ci-dessus.

Article 5 : MODALITÉS DE VERSEMENT

Sous réserve du respect par le Chef de file de ses obligations au titre du Contrat, les versements s'effectueront selon les modalités ci-après.

5.1 Avances

Jusqu'à atteindre 90 % du montant de l'aide accordée, les versements sont effectués sous forme d'avances annuelles réparties sur la durée du Projet.

Les versements sont effectués dans la limite des fonds disponibles à l'ANR suivant l'échéancier prévisionnel ci-dessous.

5.2 Solde de l'aide

Le solde de l'aide (10% du montant de l'aide accordée) est versé après présentation par le Chef de file des relevés de dépenses finaux, tels que définis à l'article 7.1.3.2, ainsi qu'après réception et validation du compte rendu de fin de Projet prévu à l'article 7.1.3.1 au plus tard dans les deux mois suivant la date d'achèvement des travaux.

Le versement du solde est ajusté pour tenir compte de la dépense réelle dans la limite du montant de l'aide.

En cas de non fourniture du relevé de dépenses final six mois après la date de fin de projet, l'analyse des dépenses sera effectuée au regard des derniers relevés de dépenses transmis à l'ANR. Si cette fourniture du relevé des dépenses est partielle, en raison de la non-transmission du relevé des dépenses par un Etablissement partenaire au Chef de file, l'ANR prendra en compte les dépenses qui auront été transmises par le Chef de file et les autres Etablissements partenaires dans le délai précité.

Dans l'éventualité d'un montant total de dépenses inférieur au cumul des versements perçus par le Chef de file, celui-ci s'engage à reverser le trop-perçu à l'État.

Les sommes versées au Chef de file au titre du Contrat ne lui sont acquises qu'au versement final ou au recouvrement du trop-perçu prévus par le Contrat.

5.3 Échéancier du versement de l'aide

Tableau récapitulatif prévisionnel pour les versements des avances pour le Projet.

Echéance	Notification (Av T0)	Av T0 + 32 mois	Solde
Total	**1 305 000 €**	**1 305 000 €**	**290 000 €**

Le versement des avances est subordonné au bon avancement du Projet et conditionné par la fourniture des documents de suivi tels que définis aux Articles 6.3, 7 et 8.

Les sommes prévues mais non versées au titre d'une année viennent augmenter l'annualité suivante, sous réserve du respect des stipulations du Contrat.

5.4 Coordonnées bancaires

Les versements prévus dans le cadre du Contrat seront effectués par l'ANR, au nom et pour le compte de l'État, sous réserve de la mise à disposition des fonds correspondants, sur le compte bancaire ouvert au nom du Chef de file :

Banque	Code banque	Code guichet	N° de compte	Clé RIB
TRESOR PUBLIC	10071	97100	00001006912	51

Cette aide n'entre pas dans le champ d'application de la TVA comme précisé à l'article 4.4 du Règlement Financier.

Article 6 : CARACTÈRE COLLECTIF DU PROJET

6.1 Partenariat

Le Projet est mené conjointement avec les Établissements partenaires indiqués en Annexe 3.

Au titre du Contrat, le Chef de file étant le seul bénéficiaire de l'aide versée par l'ANR, les autres parties prenantes du Projet ne font pas l'objet de Contrats attributifs d'aide. Les Etablissements partenaires pourront bénéficier d'un Reversement dans les conditions définies à l'Article 3 du Contrat.

6.2 Modalités de pilotage et engagements de collaboration

Le Chef de file élabore, avec l'appui du Responsable du projet et des Etablissements partenaires, les comptes rendus d'avancement à mi-parcours et de fin du Projet pour l'ensemble des travaux menés en collaboration avec les Établissements partenaires. Il assure la centralisation des relevés de dépenses et des éléments de suivi établis notamment par les Etablissements partenaires et leur bonne transmission à l'ANR.

6.3 Accord de consortium

Un accord de consortium, qui peut être constitué, après accord de l'ANR, d'un ensemble d'accords entre le Chef de file chacun des établissements partenaires individuellement, précisant les droits et obligations de chaque Établissement partenaire, au regard de la réalisation du projet, devra être fourni par le Chef de file dans un délai maximum de 12 mois à compter de la date de signature du Contrat attributif d'aide. En cas d'accords multiples, le Chef de file se porte garant de la cohérence (absence de clauses contradictoires) de cet ensemble d'accords.

L'ensemble des Établissements partenaires qui affectent des moyens au Projet sont signataires de cet accord de consortium, ou de l'accord spécifique avec le Chef de file, même s'ils ne bénéficient pas d'une quote-part de l'aide.

Cet accord de consortium rappelle l'engagement du Chef de file et des Etablissements partenaires à respecter les principes de gouvernance établis par l'action, et précise notamment selon la typologie des projets financés :

- la répartition de la dotation financière, des tâches et des livrables entre les différents partenaires, ainsi que les moyens humains et financiers mobilisés en propre par ces derniers ;
- les modalités scientifiques, techniques et financières d'accès aux ressources partagées entre les partenaires.

Le Chef de file envoie directement une copie de cet accord, ainsi que celles de ses/leurs éventuels avenants, à l'ANR.

Cet accord permettra d'évaluer l'existence éventuelle d'une aide indirecte entrant dans le calcul du taux d'aide maximum autorisé par l'encadrement des aides à la recherche, au développement et à l'innovation (RDI) (Communication de la Commission européenne n°2014/C 198/01 du 27 juin 2014) et tout texte ultérieur venant s'y substituer.

L'élaboration d'un accord de consortium n'est pas nécessaire s'il existe déjà un contrat-cadre contenant les stipulations ci-dessus liant les Établissements partenaires. Une copie de ce contrat-cadre ou une attestation devra être transmise avant la signature du Contrat attributif d'aide. À l'expiration dudit contrat, si celui-ci n'est pas reconduit, l'accord de consortium sera alors requis.

La non-transmission de ce document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'Article 11.

6.4 Respect de l'encadrement européen

L'Accord de consortium permet également de déterminer l'existence éventuelle d'une aide indirecte entrant dans le calcul du taux d'aide maximum autorisé par le régime cadre exempté de notification relatif aux aides à la recherche, au développement et à l'innovation (RDI) pour la période 2024-2026 (SA. 111723) et autres communications ou Règlements européens s'appliquant au périmètre de l'action ainsi que tout texte venant se substituer à ces règlements.

« Dans le cas de projets de coopération réalisés conjointement par des entreprises et des organismes de recherche, la Commission Européenne considère que des aides d'État indirectes ne sont pas octroyées au partenaire industriel par l'intermédiaire de l'organisme de recherche en raison des modalités favorables de la coopération si l'une des conditions suivantes est remplie :

- *les entreprises participantes supportent l'intégralité des coûts du projet ;*
- *les résultats qui ne donnent pas lieu à des droits de propriété intellectuelle peuvent être largement diffusés, et l'organisme de recherche est titulaire de tous les droits de propriété intellectuelle éventuels qui résultent de son activité de RDI ;*
- *l'organisme de recherche reçoit des entreprises participantes une rémunération équivalente au prix du marché pour les droits de propriété intellectuelle qui résultent des activités qu'il a effectuées dans le cadre du projet et qui sont transférés aux entreprises participantes. Toute contribution des entreprises participantes aux frais de l'organisme de recherche doit être déduite de ladite rémunération. ».*[1]

Article 7 : <u>OPÉRATIONS DE SUIVI ET DE FIN DE PROJET</u>

Autant que de besoin, l'ensemble des Établissements partenaires sera associé à ces opérations.

7.1 Suivi du Projet

Le Chef de file s'engage à réaliser des comptes rendus techniques et financiers de la mise en œuvre du Projet et à répondre à toutes les démarches visant à l'évaluation du Projet selon les modalités décrites dans le présent article. Il mettra, notamment, en place à cette fin un contrôle de gestion permettant à l'ANR sur la base des éléments qu'il aura transmis d'analyser l'efficience du projet, sa performance et ses résultats.

Le Chef de file s'engage également à répondre aux demandes qui pourraient lui être formulées dans le cadre d'études ou d'audits réalisés en vue du suivi et de l'évaluation *in itinere* ou *ex post* au titre de France 2030.

---

[1] Communication de la Commission du 27 juin 2014, relative à l'Encadrement des aides d'État à la recherche, au développement et à l'innovation (C198)

En particulier, il participe à toute démarche d'évaluation ou d'échanges d'expériences (colloques par exemple) mise en œuvre dans ce cadre par l'ANR.

L'ensemble des documents relatifs au suivi et fin de projet sont transmis par l'ANR au coordinateur de la stratégie nationale d'accélération.

7.1.1. Suivi annuel

7.1.1.1. Analyse d'impact

Le Chef de file renseigne annuellement les indicateurs de suivi portant sur l'état d'avancement du Projet et sur les résultats et impacts obtenus, sur une plateforme de données structurée. Ces indicateurs seront transmis au Ministère chargé de l'Enseignement Supérieur et de la Recherche, au Ministère du Travail, du Plein emploi et de l'Insertion, au Ministère de l'Education Nationale et de la Jeunesse et au Secrétariat Général Pour l'Investissement (SGPI).

Il met à disposition les données d'indicateurs de suivi demandés au plus tard le 30 septembre de chaque année à compter de l'année 2025.

La non-transmission d'un tel document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'Article 11.

7.1.1.2. Relevés de dépenses annuel

Le Chef de file adresse annuellement à l'ANR :

- un relevé récapitulatif des dépenses exécutées par chaque Établissement partenaire au cours de chaque exercice écoulé au titre du Projet, signé par le représentant légal de l'Établissement partenaire et certifié par son agent comptable ou son commissaire aux comptes, à défaut son expert-comptable ;
- les montants mis à jour des versements effectivement décaissés et prévus par les cofinanceurs pendant la durée du Projet.

Ces documents seront fournis chaque année sous format électronique au plus tard le 30 septembre de chaque année à compter de l'année 2025, à charge pour le Chef de file de conserver l'original.

La non-transmission d'un tel document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'Article 11.

7.1.2. Compte rendu à mi-parcours

Le Chef de file adresse à mi-parcours du projet, sous format électronique communiqué par l'ANR, un compte-rendu sur l'état d'avancement du Projet incluant une appréciation du degré d'atteinte des objectifs au regard des cibles initiales de résultats et d'impacts.

Ce document sera fourni au plus tard à mi-parcours.

La non-transmission d'un tel document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'Article 11.

7.1.3. Documents finaux

7.1.3.1. Compte rendu de fin de Projet

À la fin du Projet, le Chef de file adresse à l'ANR, sous format électronique communiqué par l'ANR, le compte-rendu de fin de Projet.

Ce document est transmis au plus tard dans un délai de deux (2) mois suivant la date de fin du Projet.

7.1.3.2. Relevés de dépenses finaux

À la fin du Projet, le Chef de file adresse à l'ANR :

- un relevé final des dépenses effectuées par chaque Établissement partenaire au cours de l'opération, signé par le représentant légal de l'Établissement partenaire et certifié par son agent comptable ou son commissaire aux comptes, à défaut son expert-comptable ;
- les montants mis à jour des versements effectivement décaissés par les co-financeurs pendant la durée du Projet ;
- un bilan sur les apports de chaque Établissement partenaire.

Ces documents sont transmis à l'ANR sous format électronique au plus tard dans un délai de deux mois suivant la date de fin du Projet, à charge pour le Chef de file de conserver l'original.

Tout retard ou non-transmission du compte-rendu de fin du Projet ou des relevés finaux des dépenses peut conduire au non-paiement du solde, selon les modalités de l'article 5.2 sans préjudice de l'application des stipulations de l'Article 11.

7.2 Réunions de suivi du Projet

Le coordinateur de la stratégie nationale d'accélération et les représentants des ministères sont conviés aux réunions prévues aux articles suivants.

7.2.1. Réunion de lancement

Le Responsable du projet organise une réunion de lancement du Projet avec les Établissements partenaires dans un délai de quatre (4) mois suivant la date de signature du Contrat par l'ensemble des parties. L'ANR est consultée sur la date de cette réunion au moins deux (2) mois à l'avance afin de pouvoir y participer.

7.2.2. Réunion annuelle

Le Responsable du projet organise une réunion annuelle avec les Établissements partenaires. L'ANR est consultée sur la date de cette réunion au moins un deux (2) mois à l'avance afin de pouvoir y participer.

7.2.3. Réunion de clôture

Le Responsable du projet organise une réunion de clôture du Projet avec les Établissements partenaires dans un délai de quatre mois avant la date d'achèvement du Projet. L'ANR est consultée sur la date de cette réunion au moins deux mois à l'avance afin de pouvoir y participer.

7.2.4. Suivi collectif des projets

L'ANR, le coordinateur national, ou toute autre personne désignée par le SGPI de la stratégie nationale d'accélération pourront organiser des revues de Projet, réunissant l'ensemble des Établissements partenaires et/ou Responsables des projets, pour faire un point détaillé sur l'avancement de l'action.

7.2.5. Comptes-rendus

Pour les réunions de suivi du Projet prévues aux Articles 7.2.1 à 7.2.3, un compte rendu, incluant en annexe une copie des documents présentés, doit être adressé à l'ANR ainsi qu'au coordinateur national ou toute autre personne désignée par le SGPI en version électronique sous 15 jours ouvrés à compter de la fin de la réunion.

Ce compte rendu sera également transmis au coordinateur national de la stratégie nationale d'accélération.

7.3 Évaluation in itinere et ex post

Conformément à l'Article 4 de la convention État-ANR du 8 avril 2021 susvisée, l'ANR devra procéder à une évaluation technique et socioéconomique *in itinere* et *ex post* pour apprécier l'impact des investissements consentis dans le cadre de l'action « Compétences et métiers d'avenir ».

L'ANR fera réaliser une évaluation *in itinere* pendant la durée du Projet.

L'évaluation *ex post* sera achevée au plus tard dans un délai maximum de deux ans à compter de la date de fin de Projet. Le Chef de file sera informé du choix de l'expert indépendant ou de l'organisme désigné par l'ANR. Il ne pourra le refuser que si ce choix conduit à un risque de conflit d'intérêts entre le Chef de file, les Établissements partenaires, l'expert ou l'organisme désigné.

Article 8 : PLAN DE GESTION DES DONNEES

Le Chef de file doit transmettre à l'ANR :

- un plan de gestion des données selon le modèle éventuellement fourni par l'ANR ou son propre modèle s'il en dispose dans les 12 mois suivant la signature du Contrat attributif d'aide par l'ensemble des parties ;

- une version du plan de gestion de données mise à jour à la date de fin de projet.

Lorsque la transmission d'un plan de gestion de données n'est pas justifiée au regard de l'objet du Projet décrit en Annexe 1, l'Etablissement coordinateur peut, sur demande écrite, en être dispensé par l'ANR.

La non-transmission d'un tel document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'Article 11.

Article 9 : COMMUNICATION

Sauf opposition écrite et préalable du Chef de file, le Ministère en charge de l'Enseignement Supérieur et de la Recherche, le Ministère du Travail, du Plein emploi et de l'Insertion, le Ministère de l'Education Nationale et de la Jeunesse, ou toute autre ministère dont la thématique relève de son périmètre, le Secrétariat général pour l'investissement et l'ANR pourront communiquer sur les objectifs généraux du Projet, ses enjeux et ses résultats.

Le Chef de file s'engage à participer aux opérations de communication, notamment aux colloques en cours de programme et en fin de programme organisés par l'ANR. Il en informera les Établissements partenaires.

Le Chef de file s'engage également à participer aux opérations de valorisation du plan France 2030 à la demande du Ministère en charge de l'Enseignement Supérieur et de la Recherche, du Ministère du Travail, du Plein emploi et de l'Insertion, du Ministère de l'Education Nationale et de la Jeunesse ou de tout autre représentant de l'État. Il en informera les Établissements partenaires.

Le Chef de file et les Établissements partenaires s'engagent à mentionner le soutien apporté par l'ANR au titre de France 2030, en indiquant le numéro du Contrat, dans leurs propres actions de communication sur le Projet « **CyberEDAntilles** » (ANR-24-CMAS-0014) et dans leurs publications (par exemple : « Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence « ANR-24-CMAS-0014 »). Les supports de communication orale, les communications par voie d'affiche, les sites internet doivent également afficher les logos « France 2030 ».

Les Établissements partenaires s'engagent à rendre disponible en libre accès toutes les publications scientifiques sous la licence Creative Commons CC-BY ou équivalente, en utilisant l'une des trois voies suivantes :

- publication dans une revue nativement en libre accès ;
- publication dans une revue par abonnement faisant partie d'un accord dit transformant ou journal transformatif ;
- publication dans une revue à abonnement.

La version éditeur ou le manuscrit accepté pour publication sera déposé par les auteurs dans l'archive ouverte HAL sous une licence CC- BY en mettant en œuvre la Stratégie de non-cession des droits (SNCD). De plus, le Chef de file s'engage à ce que le texte intégral de ces publications scientifiques (version acceptée pour publication ou version éditeur) soit déposé dans l'archive ouverte nationale HAL, au plus tard au moment de la publication, et à mentionner la référence ANR du projet de recherche dont elles sont issues.

Article 10 : PROTECTION DES RÉSULTATS

Dans l'hypothèse où les travaux effectués dans le cadre du Projet aidé par l'ANR aboutiraient à un dépôt de brevet ou de certificat d'utilité en France ou à l'étranger, le Chef de file doit en informer l'ANR.

Le Chef de file est tenu d'avertir l'ANR de toute cession ou nantissement du brevet en cause. Ces informations seront transmises à l'ANR sous la forme de tableaux annuels et d'un tableau récapitulatif à la clôture du projet.

Article 11 : CONDITIONS SUSPENSIVES ET DE RECOUVREMENT DE L'AIDE

En cas de difficulté de mise en œuvre, le Chef de file doit en informer l'ANR le plus rapidement possible et doit proposer un plan d'action pour y remédier.

Au cas où le Chef de file ne respecte pas les stipulations du Contrat, l'ANR, après avoir mis à même par tous moyens le Chef de file de faire valoir ses motifs, saisit le Comex. Ce dernier peut, après avis du SGPI et après que le Chef de file ait pu présenter des observations écrites ou orales, proposer soit de faire cesser le versement des tranches suivantes, soit d'interrompre le Projet et demander le recouvrement de tout ou partie des sommes versées en fonction de la gravité du manquement.

A l'exception du cas où le manquement résulte d'un manquement d'un Etablissement partenaire non imputable au Chef de file, le Contrat sera réputé faire l'objet d'un manquement grave par le Chef de file dans les cas suivants :

- mise en cause du caractère collectif du Projet tel que stipulé à l'Article 6 ;
- défaut de communication des documents justificatifs mentionnés à l'Article 5 et définis à l'Article 7 ;
- si, au vu notamment du compte rendu à mi-parcours, l'ANR constate que la capacité de le Chef de file à mener le Projet selon les modalités prévues initialement est mise en cause, ou que l'avancement du Projet présente un retard significatif par rapport au calendrier prévu ;
- inexécution partielle ou totale du Projet ;
- empêchement de faire procéder aux contrôles prévus à l'Article 6.3 du Règlement Financier, ou si ces contrôles font apparaître que tout ou partie des sommes reçues par le Chef de file n'ont pas été utilisées ou l'ont été à des fins autres que celles prévues par le Contrat ;
- manquement à l'Article 8 relatif au plan de gestion des données ;
- refus avéré et persistant de mentionner le soutien apporté par l'ANR dans les conditions définies à l'Article 9 ;
- manquement à l'Article 10 relatif à la protection des résultats.

Au cas où le non-respect des stipulations du Contrat résulte d'un manquement d'un Etablissement partenaire, l'ANR et le Chef de file s'efforcent de trouver une solution de nature à permettre la poursuite du Projet. L'ANR saisit le Comex, qui peut, après avis du SGPI et après que

l'Établissement partenaire responsable du manquement ait pu présenter des observations écrites ou orales, proposer soit que le Chef de file interrompe le versement de la quote-part de l'aide de l'Etablissement partenaire, soit que le Chef de file demande le recouvrement de tout ou partie des sommes versées à l'Etablissement partenaire, soit d'interrompre le Projet, en fonction de la gravité du manquement.

En cas de recouvrement, l'État produira un titre de recettes et effectuera le recouvrement après instruction du dossier par l'ANR.

Le Chef de file s'engage alors à reverser à l'État les montants exigés par l'ANR dans un délai de soixante jours à compter de la réception de la demande de recouvrement.

Article 12 : ENTRÉE EN VIGUEUR ET DURÉE DU CONTRAT

Le Contrat entre en vigueur à la date de sa signature par l'ensemble des parties.

Sous réserve des stipulations de l'Article 4, le Contrat prend fin à la date de règlement du solde de l'aide au Chef de file ou recouvrement du trop-perçu.

Article 13 : RÈGLEMENT FINANCIER

Le Règlement Financier relatif aux modalités d'attribution des aides des projets financés dans le cadre de l'action « Compétences et métiers d'avenir », dont le Chef de file a pris connaissance, s'applique au Contrat.

Fait à Paris, le 30 DEC. 2024 , en deux exemplaires originaux.

Pour l'Agence nationale de la recherche,	**Pour l'Université des Antilles,**
La Président-Directrice générale	Le Président
Claire GIRY	Michel GEOFFROY
	17 DEC. 2024

CAISSE D'EPARGNE
CEPAC

Ce relevé est destiné à être remis, sur leur demande, à vos créanciers ou débiteurs appelés à faire inscrire des opérations à votre compte (virement, paiement de quittance, etc.).
Son utilisation vous garantit le bon enregistrement des opérations en cause et vous évite ainsi des réclamations pour erreurs ou retards d'imputation.

11315	00001	08028147507	17	CE CEPAC
c/étab	*c/guichet*	*n/compte*	*c/rice*	*domiciliation*

IBAN

FR76	1131	5000	0108	0281	4750	717

BIC

C	E	P	A	F	R	P	P	1	3	1

Intitulé du compte **AGENCE CARIBEENNE POUR LA CYBER**
189 RUE VICTOR MAMADO
97128 GOYAVE

LE GOSIER
IMMEUBLE PLAZA MONTAUBAN
97190 LE GOSIER
Tél.: 32.41. . .

CAISSE D'EPARGNE
CEPAC

Ce relevé est destiné à être remis, sur leur demande, à vos créanciers ou débiteurs appelés à faire inscrire des opérations à votre compte (virement, paiement de quittance, etc.).
Son utilisation vous garantit le bon enregistrement des opérations en cause et vous évite ainsi des réclamations pour erreurs ou retards d'imputation.

11315	00001	08028147507	17	CE CEPAC
c/étab	*c/guichet*	*n/compte*	*c/rice*	*domiciliation*

IBAN

FR76	1131	5000	0108	0281	4750	717

BIC

C	E	P	A	F	R	P	P	1	3	1

Intitulé du compte **AGENCE CARIBEENNE POUR LA CYBER**
189 RUE VICTOR MAMADO
97128 GOYAVE

LE GOSIER
IMMEUBLE PLAZA MONTAUBAN
97190 LE GOSIER
Tél.: 32.41. . .

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

anr agence nationale de la recherche

FRANCE 2030

Fait à Paris, le 01 SEP. 2025

DÉCISION COLLECTIVE

La Présidente directrice générale de l'Agence Nationale de la Recherche :

Vu les contrats attributifs d'aide cités en annexe ;

DÉCIDE :

ARTICLE UN

Un alinéa est ajouté à l'article 3 intitulé « Montant et gestion de l'aide » des contrats attributifs d'aide cités en annexe :

Pour les Entreprises bénéficiaires d'un Reversement, l'Etablissement coordinateur veille à ce que l'échéancier de reversement soit annualisé et corresponde aux besoins de financement effectifs pour chaque exercice considéré, et à ce que les conventions de Reversement prévoient une clause de suspension du Reversement de l'aide en cas de doute sur la solidité financière ou de défaillance de l'Entreprise.

ARTICLE DEUX

L'article 7.1.1.3 intitulé « Suivi de la situation financière des Entreprises bénéficiaires » est ajouté aux contrats attributifs d'aide cités en annexe :

Les Etablissements partenaires ayant la qualité d'Entreprise (au sens de l'Article 1) et bénéficiant du Reversement d'une quote-part de l'aide sont tenus de transmettre à l'ANR le bilan comptable relatif à l'exercice précédent (année n-1), au plus tard le 30 juin de chaque année à compter de l'année 2025. L'Etablissement coordinateur veille à la bonne transmission de ces documents,

notamment en transcrivant cette obligation dans les conventions de Reversement mentionnées à l'Article 3 et/ou dans l'Accord de consortium visé à l'Article 6.3.

La non-transmission d'un tel document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'Article 11.

Si l'Etablissement coordinateur a connaissance d'une information sur la situation d'une Entreprise partenaire bénéficiaire mettant en cause sa solidité financière, il doit en alerter l'ANR dans les plus brefs délais.

Si l'ANR estime que la solidité financière de l'Entreprise partenaire ne lui permet pas d'assurer la contrepartie nécessaire à la réalisation du Projet, elle peut mettre en œuvre la procédure de suspension et de recouvrement de l'aide prévue à l'Article 11.

ARTICLE TROIS

Dans l'article 11 intitulé « Conditions suspensives et de recouvrement de l'aide » des contrats attributifs d'aide cités en annexe est ajouté à l'alinéa 3 :

- *si, au regard des documents comptables transmis à l'ANR conformément à l'Article 7.1.1.3, il apparaît que la solidité financière d'un Etablissement partenaire privé bénéficiaire d'un Reversement ne lui permet pas d'assurer la contrepartie financière nécessaire à la réalisation du Projet*

La Présidente directrice générale de l'Agence Nationale de la Recherche

Claire GIRY

ANNEXE

22-CMAS-0001	QuanTEdu-France
22-CMAS-0003	EFELIA-ANITI
22-CMAS-0004	EFELIA Côte d'Azur
22-CMAS-0005	EFELIA-MIAI
22-CMAS-0006	SORBONNE.AI
22-CMAS-0007	EFELIA-PRAIRIE
22-CMAS-0008	SaclAI School
22-CMAS-0009	CAPS'UL
22-CMAS-0010	DINUSA
22-CMAS-0011	ECSN
22-CMAS-0012	ESNbyUM
22-CMAS-0013	FURII-DEM@TER
22-CMAS-0014	SaNu-RN
22-CMAS-0015	SATIN
22-CMAS-0016	SNB22
22-CMAS-0017	amàRéno
22-CMAS-0018	GENHYO
22-CMAS-0019	Digital FCU
22-CMAS-0020	MANU
22-CMAS-0021	CyberSkills@UGA
22-CMAS-0022	AMHY de Grenoble
23-CMAS-0001	1H-EID
23-CMAS-0002	ARCliMed
23-CMAS-0003	AVID
23-CMAS-0004	Bio'Occ
23-CMAS-0005	CINERG'e-santé
23-CMAS-0006	EID@Lyon
23-CMAS-0007	ESOS

23-CMAS-0008	Fo6Med
23-CMAS-0009	IBES
23-CMAS-0010	NORMANTHIIA
23-CMAS-0011	NSM5P
23-CMAS-0012	SENS (CMA)
23-CMAS-0013	SN@SU
23-CMAS-0014	TCE
23-CMAS-0015	TETP
23-CMAS-0016	TIARe
23-CMAS-0017	UB2030 - CAP IA
23-CMAS-0018	UB2030 - CAP Santé Numérique
23-CMAS-0019	CyberINSA
23-CMAS-0020	TAL-CYB
23-CMAS-0021	UB2030-CAP ELENA
23-CMAS-0022	FAME
23-CMAS-0023	RIS3
23-CMAS-0024	INFORISM
23-CMAS-0025	FAMOUS
23-CMAS-0026	CyberSkills4All
23-CMAS-0027	CYRCE
23-CMAS-0028	C-DéCIDé
23-CMAS-0029	DecarboChim
23-CMAS-0030	HTASE
23-CMAS-0031	CAIRE
23-CMAS-0032	BIOT2@Normandie
23-CMAS-0033	DaTSHealth
23-CMAS-0034	DigiHealth Paris Cité
23-CMAS-0035	PFDS
23-CMAS-0036	EDSAN
23-CMAS-0037	PariSantéNum
23-CMAS-0038	PROMESS
23-CMAS-0039	ReDHI

23-CMAS-0040	UNIVEReSANTE
23-CMAS-0041	SPACE-IDF
23-CMAS-0042	LaTêteDanslesNuages@UGA
24-CMAS-0001	UNITEID
24-CMAS-0002	AMUS@N-NUM
24-CMAS-0003	OFFWIND
24-CMAS-0004	BIORAF
24-CMAS-0005	EESL
24-CMAS-0006	PRIMANS
24-CMAS-0007	AISorb
24-CMAS-0008	MERCASTO
24-CMAS-0009	ENSUIITE
24-CMAS-0010	NumiaCare-Saclay
24-CMAS-0011	I-BE3 (PSL BoE)
24-CMAS-0012	CMA Chimie Verte Academy
24-CMAS-0013	Penso
24-CMAS-0014	CyberEDAntilles
24-CMAS-0015	COMETES
24-CMAS-0019	Exa2Bio

CONVENTION DE REVERSEMENT DE FONDS

Projet ANR CyberEDANtilles (ANR-24-CMAS-0014)

L'Université des Antilles
Etablissement public à caractère scientifique, culturel et professionnel (EPSCP)
Référencée sous le numéro SIRET 199 715 855 00011
Située au Campus de Fouillole, BP 250, 97175 Pointe-à-Pitre, Guadeloupe

Représentée par son Président, Monsieur Michel GEOFFROY,

Ci-après dénommée par « UA » ou « le Chef de file »

D'une part,

ET

ENTRE

Association Agence Caribéenne pour la Cybersécurité (ACCYB),
Association enregistrée au registre des associations W9G1011279 au Code APE 94.99Z
Référencé sous le numéro SIRET : 918 714 890 00012
Situé 189, rue Victor Mamado, 97128 Goyave, Guadeloupe

Représentée par sa Présidente, Madame Marie-Lucienne RATTIER,

ci-après dénommée par « ACCYB » ou « l'Etablissement partenaire »

D'autre part,

L'UA et l'Etablissement partenaire pouvant ci-après être dénommés individuellement par la « **Partie** » ou collectivement par les « **Parties** »
VISA :

Vu le décret n° 2006-963 du 1er août 2006 modifié portant organisation et fonctionnement de l'Agence Nationale de la Recherche ;
Vu la loi de finances rectificative n°2010-237 du 9 mars 2010 de finances rectificatives pour 2010, notamment son article 8 ;
Vu la convention du 8 avril 2021 modifiée entre l'État, l'ADEME, l'Agence nationale de la recherche, la

HLR

Caisse des dépôts et consignations, l'EPIC Bpifrance et la société anonyme Bpifrance encadrant les dispositions communes aux conventions relatives à la mise en œuvre du quatrième programme d'investissements d'avenir et du plan France 2030 ;
Vu la convention du 4 juin 2021 entre l'État, l'ADEME, l'Agence nationale de la recherche, la Caisse des dépôts et consignations, l'EPIC Bpifrance et la société anonyme Bpifrance relative au programme d'investissements d'avenir (action « Soutien au déploiement ») ;
Vu l'arrêté du 11 mai 2023 relatif à l'approbation du cahier des charges de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » ;
Vu le règlement financier relatif aux modalités d'attribution des aides au titre de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » ;
Vu la décision n° 2024-DEPL-062431 du Premier Ministre, en date du 3 juillet 2024, autorisant l'ANR à contractualiser avec le Chef de file sur le financement du Projet « CyberEDAntilles » dans le cadre de l'action « Compétences et métiers d'avenir » ;
Vu le contrat attributif d'aide n° ANR-24-CMAS-0014 entrée en vigueur le 1er janvier 2025, signé entre l'UA et l'ANR relative au financement du projet « CyberEDAntilles » par l'ANR.

IL EST CONVENU DE CE QUI SUIT :

ARTICLE 1 – DÉFINITIONS

Les termes ou expressions ci-après, tant au singulier qu'au pluriel, auront les significations suivantes dans la présente Convention chaque fois qu'ils apparaîtront.

Responsable de Projet : personne physique qui assure la coordination du projet pour le compte du Chef de file.

Chef de file : Établissement porteur, doté de la personnalité morale, il est l'interlocuteur privilégié de l'Opérateur pour les aspects administratifs et financiers. Il désigne l'UA dans le cadre de cette présente convention. Il est responsable de la mise en place et de la formalisation de la collaboration entre les Établissements partenaires, de la production des livrables du projet, de la tenue des réunions d'avancement et de la communication des résultats. Il s'appuie pour cela sur le Responsable du projet.

Établissement partenaire : c'est un des organismes de formation ou d'accompagnement, des employeurs ou leurs représentants, des collectivités territoriales, parties prenantes au projet.
Chacun des Établissements partenaires désigne en son sein un correspondant du Responsable du projet.

Établissement gestionnaire : établissement partenaire du projet différent du Chef de file choisi, le cas échéant, conformément aux délégations de gestion en vigueur existant entre les Établissements publics partenaires impliqués dans le projet. L'Établissement gestionnaire de l'aide est doté de la personnalité morale.

Contrat attributif : désigne le contrat attributif d'aide n°ANR-24-CMAS-0014 entrée en vigueur le 1er janvier 2025, signé entre l'ANR et l'UA, relatif au financement du projet CyberEDAntilles par l'ANR ainsi que ses annexes.

Convention : désigne la présente convention de reversement.

Reversement : quote-part de l'aide versée par le chef de file à l'Établissement partenaire en vertu de la présente Convention de reversement, pour la réalisation d'une tâche ou d'une mission dans le cadre

HLR

du projet, dans le respect de l'encadrement européen des aides.

Règlement financier : règlement relatif aux modalités d'attribution des aides au titre de l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » daté du 22 décembre 2021 et mis à jour le 30 juin 2025. Il s'applique à la Convention de reversement et l'Etablissement partenaire est réputé en avoir pris connaissance et y avoir adhéré.

Projet : le projet CyberEDAntilles a été retenu par l'ANR par décision n° 2024-DEPL-062431 du Premier Ministre, en date du 3 juillet 2024, et la description scientifique figure dans l'annexe 1 du contrat attributif d'aide. La date de commencement du Projet et sa durée de réalisation sont fixées dans le contrat attributif d'aide.

Consortium ou groupement : Le groupement est composé de partenaires souhaitant répondre conjointement à l'appel à manifestation d'intérêt afin d'apporter une réponse commune aux enjeux identifiés. Ce sont des partenaires opérationnels du projet qui mettent en œuvre des moyens qui leur sont propres. Le groupement est représenté par un chef de file (le porteur de projet) auquel les autres membres du groupement donnent expressément mandat pour les représenter dans le cadre du projet. Les membres du groupement concluent un accord de consortium prévoyant, notamment, la gouvernance du projet, ses objectifs et les moyens mis en œuvre.

Encadrement européen : l'aide versée est susceptible de constituer une aide d'Etat au sens de l'article 107, §1 du TFUE si elle soutient des activités économiques entendu comme toute offre de biens ou des services sur un marché donné. Les bases juridiques mobilisables sont : l'Encadrement des Aides d'Etat à la recherche, au développement et à l'innovation n°2022/C 414/01 du 28 octobre 2022 ou toute communication ultérieure venant s'y substituer, le régime cadre exempté n° SA. 111723 d'aides à la recherche, au développement et à l'innovation pris sur la base du règlement général d'exemption par catégorie n° 651/2014 adopté par la Commission européenne le 17 juin 2014 et publié au JOUE le 26 juin 2014, tel que modifié par les Règlements (UE) 2017/1084 de la Commission du 14 juin 2017, publié au Journal Officiel de l'Union Européenne du 20 juin 2017, 2020/972 du 2 juillet 2020 publié au JOUE du 7 juillet 2020 et 2023/1315 du 23 juin 2023 publié au JOUE du 30 juin 2023 ou tout autre régime cadre exempté validé par la Commission européenne, le règlement n° 2023/2831 de la Commission du 13 décembre 2023 « relatif à l'application des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne aux aides de minimis de minimis » et la décision de la Commission du 20 décembre 2011 « relative à l'application de l'article 106, paragraphe 2, du traité sur le fonctionnement de l'Union européenne aux aides d'État sous forme de compensations de service public octroyées à certaines entreprises chargées de la gestion de services d'intérêt économique général ».

Entreprise : au sens de la règlementation européenne sur les aides d'Etat, « est considérée comme entreprise toute entité, indépendamment de sa forme juridique, exerçant une activité économique ». Selon leur taille et leur importance économique, ces entités sont classées selon les trois catégories suivantes : les grandes entreprises, les petites et moyennes entreprises (PME). La définition des petites et moyennes entreprises (PME) est celle de l'Annexe 1 du Règlement (CE) n° 651/2014 de la Commission Européenne du 17 juin 2014 et figure dans la recommandation 2003/ 361/CE de la Commission Européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises et tout texte communautaire venant s'y substituer

ARTICLE 2 – OBJET

L'objet de la présente Convention de reversement est de définir les conditions et les modalités de reversement de la quote-part de l'aide par le Chef de file à l'Etablissement partenaire.

L'Etablissement partenaire s'engage à réaliser, dans les délais stipulés à l'article 4 de la présente Convention, les tâches lui incombant dans le cadre du Projet dont le descriptif figure à l'annexe n°1 et le budget à l'annexe 2 de la présente Convention.

L'Etablissement partenaire réalise ces tâches en étroite collaboration avec le Chef de file et avec les autres Etablissements partenaires impliqués dans le Projet, dont la liste figure à l'annexe n°3 de la présente Convention.

ARTICLE 3 – COORDINATION DU PROJET

Les responsables dédiés à la réalisation du Projet sont :

- Pour le Chef de file : Pr. Erick Stattner, Directeur du Département Mathématiques-Informatique (DMI) et responsable du Master MIAGE (Méthodes Informatiques Appliquées à la Gestion des Entreprises)

- Pour l'Etablissement Partenaire : Mme Marie-Lucienne RATTIER, Présidente de l'ACCYB

L'Etablissement partenaire s'engage à collaborer avec le Chef de file afin que celui-ci puisse assurer vis-à-vis de l'Organisme financeur l'exécution de ses différentes obligations, et notamment le suivi annuel, l'élaboration des comptes rendus à mi-parcours et de fin de projet pour l'ensemble des travaux menés en collaboration avec le Chef de file et les autres Établissements partenaires.

Le Chef de file élabore, avec l'appui du Responsable du projet et des Etablissements partenaires, les comptes rendus d'avancement à mi-parcours et de fin du Projet pour l'ensemble des travaux menés en collaboration avec les Établissements partenaires.

ARTICLE 4 – PRISE D'EFFET –DUREE

La présente Convention de reversement prendra effet à la date de sa signature.
La date de démarrage du Projet et de prise en compte des dépenses est fixée au 01/01/2025.
La durée de réalisation du Projet est fixée à 60 mois, soit un achèvement prévu à la date du 31/12/2029 qui correspond à celle de fin de prise en compte des dépenses.

Sauf résiliation de la Convention de reversement conformément à l'article 8 ci-après, cette Convention prend fin à la date de règlement du solde de la quote-part de l'aide à l'Etablissement partenaire par le Chef de file ou à la date du recouvrement du trop-perçu de paiement de l'Etablissement partenaire au Chef de file.

ARTICLE 5 – OBLIGATIONS DE L'ETABLISSEMENT PARTENAIRE

5.1 Au titre de la Convention de reversement, l'Etablissement partenaire s'engage à :

- Affecter la quote-part de l'aide versée par le Chef de file à la réalisation exclusive de sa part du

projet et des activités qui lui incombent, sous réserve des dispositions de l'article 3.1 du Règlement financier relatif aux dépenses éligibles ;

- Respecter l'échéancier des opérations d'acquisition et des opérations de fonctionnement pour sa part du projet ;
- Réaliser les activités du projet avec la participation des autres partenaires et dans les délais définis à l'article 4 de la Convention de reversement et conformément à l'annexe 1 de la présente Convention ;
- Participer aux réunions de suivi du projet (lancement, réunions annuelles et clôture) ;
- Répondre aux demandes du Chef de file qui pourraient lui être formulées dans le cadre d'études ou d'audits réalisés en vue du suivi et de l'évaluation in itinere ou ex post au titre de France 2030 ;
- Mentionner le soutien apporté par l'ANR au titre de France 2030, en indiquant le numéro du Contrat, dans leurs propres actions de communication sur le Projet « CyberEDAntilles » (ANR-24-CMAS-0014) et dans leurs publications (par exemple : « Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence « ANR-24-CMAS-0014 »). Les supports de communication orale, les communications par voie d'affiche, les sites internet doivent également afficher les logos « France 2030 » ;
- Rendre disponible en libre accès toutes les publications scientifiques sous la licence Creative Commons CC-BY ou équivalente, en utilisant l'une des trois voies suivantes :
  - publication dans une revue nativement en libre accès ;
  - publication dans une revue par abonnement faisant partie d'un accord dit transformant ou journal transformatif ;
  - publication dans une revue à abonnement ;
- Dans l'hypothèse où les travaux effectués dans le cadre du Projet aidé par l'ANR aboutiraient à un dépôt de brevet ou de certificat d'utilité en France ou à l'étranger, l'établissement partenaire doit en informer le Chef de file. L'établissement partenaire est tenu d'avertir le Chef de file de toute cession ou nantissement du brevet en cause ;
- Informer le plus rapidement possible le Chef de file de toute difficulté de mise en œuvre de sa part du projet.

5.2 L'Etablissement partenaire s'engage à transmettre au Chef de file, dans les délais imposés par l'ANR dans le contrat attributif d'aide, tous les éléments permettant à ce dernier de renseigner les documents de suivi annuel (analyse de l'impact et relevés de dépenses), le compte-rendu à mi-parcours et les documents finaux (compte-rendu de fin de projet et relevés des dépenses finaux).

A ce titre, l'Etablissement partenaire :

- transmettra au chef de file les indicateurs de suivi de ses actions au plus tard le 31 août de chaque année pour que le Chef de file puisse renseigner annuellement les indicateurs de suivi portant sur l'état d'avancement du Projet et sur les résultats et impacts obtenus, sur la plateforme de données dédiée au plus tard le 30 septembre.
- désignera un référent financier qui sera chargé de renseigner les dépenses effectuées de juillet N-1 à juin sur la plateforme dédiée au plus tard le 07 septembre de chaque année. Le Chef de file vérifiera ce relevé de dépense annuel saisi. Une fois qu'il l'aura validé, ce document pourra être signé par le représentant légal de l'Établissement partenaire et certifié par son agent comptable ou son commissaire aux comptes, à défaut son expert-comptable. Le Chef de file mettra ce document en ligne avec celui des autres Etablissements partenaires au plus tard le 30 septembre de chaque année.
  Le référent financier de l'Etablissement partenaire saisira également sur la plateforme dédiée

le relevé final des dépenses de l'Etablissement partenaire sur le projet au plus tard le 07 février 2030. Le Chef de file vérifiera ce relevé de dépense final saisi. Une fois validé, ce dernier pourra être signé par le représentant légal de l'Établissement partenaire et certifié par son agent comptable ou son commissaire aux comptes, à défaut son expert-comptable. Le Chef de file mettra ce document en ligne avec celui des autres Etablissements partenaires dans un délai de deux mois suivant la date de fin du Projet.

5.3 Suivi de la situation financière de l'établissement partenaire ayant la qualité d'entreprise

Orange Antilles-Guyane ayant la qualité d'entreprise (au sens de l'article 1) et bénéficiant de reversement d'une quote-part de l'aide est tenu de transmettre à l'ANR, par l'intermédiaire du Chef de fil le bilan comptable relatif à l'exercice précédent (année n-1), *au plus tard le 30 juin de chaque année* à compter de l'année 2025. La non-transmission d'un tel document peut conduire à l'interruption du versement de l'aide conformément aux stipulations prévues à l'article 11 du contrat attributif.

ARTICLE 6 – MONTANT DE L'AIDE ET MODALITES DE REVERSEMENT

Sous réserve de la mise à disposition effective des fonds au Chef de file, de l'absence de mise en œuvre de l'article 8 de la présente Convention et du respect par l'Etablissement partenaire de ses obligations au titre de la Convention de reversement, le Chef de file s'engage à verser à l'Etablissement partenaire la quote-part de l'aide d'un montant maximal de 12 890 euros [douze mille huit cent quatre-vingt-dix euros] selon les modalités ci-après.

6.1 Avances

Jusqu'à atteindre 90 % du montant de l'aide accordée, les versements sont effectués sous forme d'avances réparties sur la durée du Projet.
Les versements sont effectués dans la limite du montant maximum accordé à l'Etablissement partenaire dans le cadre du projet et suivant l'échéancier prévisionnel ci-dessous.

A l'exception du premier versement qui est effectué à la signature de la Convention de reversement, les versements suivants seront soumis à la validation des éléments attendus de la part de l'Etablissement partenaire par le Chef de file pour que celui-ci puisse produire les documents de suivi annuel (analyse de l'impact et relevés de dépenses), le compte-rendu à mi-parcours et les documents finaux (compte-rendu de fin de projet et relevés des dépenses finaux).

La validation des éléments attendus reposera également sur la conformité des dépenses éligibles de l'Etablissement partenaire à celles établies pour la période concernée dans le budget validé et financé décrit à l'annexe 2.

Si un changement est envisagé dans la répartition entre les postes de dépenses, il conviendra de tenir informé le Chef de file et de recueillir sa validation avant tout changement.

6.2 Solde de la quote-part de l'aide

Conformément aux stipulations de l'article 5.2 de la présente Convention de reversement, le Chef de file procédera à la consolidation des éléments constituants les documents finaux (compte-rendu de fin de projet et relevés des dépenses finaux), pour une transmission à l'ANR au plus tard dans un délai de deux (2) mois suivant la date de fin de projet.
L'ANR procédera au versement du solde au Chef de file avec un ajustement éventuel pour tenir compte de la dépense réelle dans la limite du montant de l'aide attribuée et selon les stipulations de l'article 5.2 du contrat attributif d'aide.

Le Chef de file procédera au versement du solde de la quote-part de l'aide à l'Etablissement partenaire dans des conditions similaires :

- Le versement du solde de la quote-part de l'aide à l'Etablissement partenaire sera ajusté pour tenir compte de la dépense réelle dans la limite de la quote-part de l'aide prévue ;
- En cas de non-transmission du relevé final des dépenses de l'Etablissement partenaire dans les délais, l'analyse des dépenses sera effectuée au regard des derniers relevés de dépenses transmis par l'Etablissement partenaire au Chef de file ;
- Dans l'éventualité d'un montant total de dépenses inférieur au cumul des versements perçus par l'Etablissement partenaire, celui-ci s'engage à reverser le trop-perçu au Chef de file ;
- Les sommes versées à l'Etablissement partenaire au titre de la Convention de reversement ne lui sont acquises qu'au versement final ou au recouvrement du trop-perçu prévus par la Convention.

6.3 Échéancier du versement de la quote-part de l'aide

Pour les entreprises bénéficiaires d'un reversement, le Chef de file veille à ce que l'échéancier de reversement soit annualisé et corresponde aux besoins de financement effectifs pour chaque exercice considéré, et à ce que les conventions de reversement prévoient une clause de suspension du reversement de l'aide en cas de solidité financière ou de défaillance de l'entreprise.

Tableau récapitulatif prévisionnel pour les versements des avances pour le Projet.

Echéance	Signature de la convention de reversement	2026	2027	2028	Solde
Total quote-part de l'aide à l'Etablissement partenaire	**13 689,00 €**	**62 603,28 €**	**67 984,24 €**	**31 984,24 €**	**27 499,24 €**

Le versement des avances est subordonné au bon avancement du Projet et conditionné par la fourniture des documents de suivi tels que définis à l'Article 5.2 et Article 7.
Les sommes prévues mais non versées au titre d'une année viennent augmenter l'annualité suivante, sous réserve du respect des stipulations de la Convention.

HLR

6.4 Coordonnées bancaires

Les versements prévus dans le cadre de la Convention seront effectués par le Chef de file, sous réserve de la mise à disposition des fonds correspondants par l'ANR, sur le compte bancaire ouvert au nom de l'Agent Comptable de : **Association Agence caribéenne pour la cybersécurité.**

Au nom de : Association Agence caribéenne pour la cybersécurité				
Domiciliation	**Code Banque**	**Code Guichet**	**N° de Compte**	**Clé RIB**
CE CEPAC	**11315**	**00001**	**0802847507**	**717**

Le RIB est annexé à la présente Convention (annexe 5), sur présentation d'une facture adressée par l'Etablissement Partenaire au chef de file sur Chorus pro.

ARTICLE 7 : CONDITIONS SUSPENSIVES ET DE RESTITUTION DE LA QUOTE-PART DE L'AIDE

En cas de difficulté de mise en œuvre, l'Etablissement partenaire doit en informer le Chef de file le plus rapidement possible et doit proposer un plan d'action pour y remédier.

Au regard de l'article 3 de la nouvelle Décision collective de l'ANR en date du 01 septembre 2025 relative à l'analyse de la santé financière de l'entreprise partenaire et bénéficiaire, si les documents comptables transmis à l'ANR font apparaître une déficience financière de l'établissement partenaire privé bénéficiaire d'un reversement ne lui permettant pas d'assurer la contrepartie financière nécessaire à la réalisation du projet, l'ANR peut mettre en œuvre la procédure de suspension et de recouvrement de l'aide.

Dans l'hypothèse où l'ANR, pour quelque raison que ce soit, suspendrait ou cesserait le versement de l'Aide, le Chef de file pourra suspendre ou cesser le versement de la quote-part de l'aide à l'Etablissement partenaire.

Dans l'hypothèse où l'ANR, pour quelque cause que ce soit, demanderait la restitution de tout ou partie de l'aide, l'Etablissement partenaire s'engage à reverser au Chef de file tout ou partie de sa quote-part de l'aide, dans des proportions indiquées par le Chef de file, dans un délai de trente (30) jours à compter de la réception de la demande de recouvrement du Chef de file.

Le Chef de file s'engage à communiquer à l'Etablissement partenaire tout document justifiant ces opérations.

L'utilisation de la subvention perçue à des fins autres que celles définies dans ledit Contrat attributif ainsi que dans la présente Convention entraînera, le remboursement du montant total au Chef de file de la subvention qui lui aura été versée.

Au cas où le non-respect des stipulations du Contrat attributif d'aide résulte d'un manquement de l'Etablissement partenaire, l'ANR et le Chef de file s'efforcent de trouver une solution de nature à permettre la poursuite du Projet. L'ANR saisit le Comex, qui peut, après avis du SGPI et après que l'Établissement partenaire responsable du manquement ait pu présenter des observations écrites,

proposer soit que le Chef de file interrompe le versement de la quote-part de l'aide de l'Etablissement partenaire, soit que le Chef de file demande le recouvrement de tout ou partie des sommes versées à l'Etablissement partenaire, soit d'interrompre le Projet, en fonction de la gravité du manquement.

La cessation du versement de la quote-part de l'aide ou la restitution de la quote-part de l'aide entrainent la résiliation de la Convention de reversement.

ARTICLE 8 - RESILIATION DE LA CONVENTION

La présente convention pourra être résiliée de plein droit par l'une quelconque des Parties en cas d'inexécution par l'autre Partie d'une ou plusieurs des obligations contenues dans ses diverses clauses. Cette résiliation ne deviendra effective que trois (3) mois après une mise en demeure exposant les motifs de la plainte, adressée par la Partie plaignante à la Partie défaillante par courrier recommandé, à moins que dans ce délai, la Partie défaillante n'ait satisfait à ses obligations ou n'ait apporté la preuve d'un empêchement consécutif à un cas de force majeure.

L'exercice de cette faculté de résiliation ne dispense pas la Partie défaillante de remplir les obligations contractées jusqu'à la date d'effet de la résiliation et ce, sans préjudice des indemnités auxquelles la Partie plaignante pourrait avoir droit en raison des dommages éventuellement subis du fait de la rupture anticipée de la Convention.

Une telle résiliation n'aura pas pour effet de libérer l'Etablissement partenaire de l'obligation d'exécution des Travaux et de remise des rapports prévus jusqu'à la date de résiliation.

ARTICLE 9 – LOI APPLICABLE ET DIFFERENDS

La présente Convention est soumise, pour sa validité, son interprétation et en cas de litige dans son exécution, à la législation française.
En cas de litige survenant entre les Parties au sujet de l'existence, la validité, l'interprétation, l'exécution ou la rupture de la présente Convention, les Parties s'engagent à se rencontrer, à l'initiative de la Partie la plus diligente, et à mettre en œuvre tous les moyens pour résoudre le litige de façon amiable avant tout recours juridictionnel ; les Responsables Scientifiques et/ou les représentants de chaque Partie proposent à cet effet toute solution de conciliation.

Le défaut d'accord à l'issue d'un délai d'un (1) mois à compter de sa constatation notifiée par courrier recommandé, par l'une des Parties à l'autre Partie, vaudra échec desdites négociations. La preuve du début des négociations ne pourra être rapportée que la rédaction d'un procès-verbal de réunion rédigé en (3) trois exemplaires, dûment signé par les représentants des Parties.

En cas d'échec des négociations, le litige sera porté devant les tribunaux français compétents.

ARTICLE 10 - DISPOSITIONS GENERALES

Cession
La présente convention est conclue *intuitu personae* ; par conséquent, aucune des Parties ne pourra transférer de quelque façon que ce soit les droits d'obligations y afférent sans le consentement

préalable de l'autre Partie.

Invalidité d'une clause
Si une ou plusieurs stipulations de la présente convention étaient tenues pour non valides ou déclarées telles en application d'un traité, d'une loi ou d'un règlement, ou encore à la suite de la décision définitive d'une juridiction compétente, les autres stipulations garderont toute leur force et leur portée. Les Parties procéderont alors sans délai aux modifications nécessaires en respectant, dans toute la mesure du possible, l'équilibre des droits et obligations de chacune conformément à l'accord de volonté existant au moment de la signature de la présente Convention.

ARTICLE 11- PIECES CONTRACTUELLES

Font partie intégrante de la Convention, le présent document et ses annexes, à savoir :
- Annexe 1 : Descriptif du Projet ;
- Annexe 2 : Document administratif et financier ;
- Annexe 3 : Partenaires et responsable de projet ;
- Annexe 4 : Contrat attributif d'aide conclu entre l'ANR et le Chef de file ;
- Annexe 5 : RIB de l'Etablissement partenaire ;
- Annexe 6 : Nouvelle décision collective de l'ANR du 01 septembre 2025.

Fait en deux (2) exemplaires originaux

Pour l'ACCYB
Le : 10/11/2025

La Présidente

Marie-Lucienne RATTIER

Pour L'UA
Le : 13 FEV. 2026

Le Président

Pr. Michel GEOFFROY

AGENCE CARIBÉENNE POUR LA CYBERSÉCURITÉ

ACCYB

Classification: **Réservé**

Petit-Bourg, le 05 janvier 2026

Président

LETTRE

destinataires

in fine

Madame, Monsieur,

Conformément à l'article 9.4 des statuts de l'Agence Caribéenne pour la Cybersécurité (ACCYB), prévoyant une **présidence tournante entre les Collectivités Territoriales Chef de File pour une durée de douze mois**, j'ai l'honneur de vous informer que **Monsieur Steven COCKS**, **Conseiller territorial de la Collectivité d'Outre-mer de Saint-Martin**, assure désormais la présidence de l'Association.

Cette prise de fonction s'inscrit dans le cadre de la **délibération territoriale du 4 février 2022**, par laquelle la Collectivité a confirmé son engagement en qualité de membre de droit et son rôle renforcé dans la gouvernance de l'ACCYB.

Sous la présidence de Monsieur COCKS, l'Association poursuivra, en lien étroit avec les services de l'État, ses missions essentielles : coordination opérationnelle, appui aux acteurs publics et privés, partage d'informations de cybersécurité et accompagnement des initiatives visant à renforcer la résilience numérique des territoires français d'Amérique.

Je vous remercie de bien vouloir prendre acte de cette évolution institutionnelle et me tiens à votre disposition pour tout échange concernant les priorités stratégiques de l'Association.

Veuillez agréer, Madame, Monsieur, l'expression de ma considération distinguée.

Monsieur Steven COCKS
Président de Agence caribéenne pour la cybersécurité
Conseiller territorial de la Collectivité d'Outre-mer de Saint-Martin

Destinataires :
Madame la directrice générale des outre-mer, Anne-Gaëlle BAUDOUIN
Monsieur le directeur général de l'Agence nationale de la sécurité des systèmes d'information, Vincent STRUBEL
Monsieur le Préfet de la région Guadeloupe, Thierry DEVIMEUX
Monsieur le Préfet de la région Guyane, Antoine POUSSIER
Monsieur le Préfet de la région Martinique, Étienne DESPLANQUES
Monsieur le Préfet de Saint-Barthélemy et de Saint- Martin, Cyrille LE VELY
Monsieur le Préfet de Saint-Pierre et Miquelon, Marc DIDIO

Statuts

ARTICLE 1. CONSTITUTION

Il est fondé entre les adhérents aux présents statuts une Association régie par la Loi du 1er juillet 1901, son décret d'application du 16 Août 1901 et les présents statuts.

ARTICLE 2. DENOMINATION

La dénomination sociale de cette Association est « Agence Caribéenne pour la Cybersécurité ».

ARTICLE 3. OBJET

Face aux défis posés par la transformation numérique, l'Association a pour but de favoriser, par tous moyens, les échanges de connaissances entre les sphères scientifique, économique et publique, ainsi que l'émergence de solutions de long terme regardant la cybersécurité, la sûreté et la résilience des territoires français d'Amérique et de la zone Caraïbes.

ARTICLE 4. SIEGE SOCIAL

Le siège de l'Association est fixé au 189 rue Victor Mamado, Fort Isle, à Goyave (97128). Il peut être transféré sur simple décision du Conseil d'Administration.

ARTICLE 5. DUREE

La durée de l'Association est illimitée.

ARTICLE 6. COMPOSITION

L'Association se compose de huit catégories de membres :

- les membres « **Collectivités Territoriales Chef de file** », comprennent les collectivités régies par l'article 74 de la constitution ainsi que les collectivités régionales ou territoriales qui portent une compétence exclusive pour définir les orientations en matière de développement économique sur leurs territoires respectifs au titre de la loi portant sur la Nouvelle Organisation Territoriale de la République (NOTRe). Elles sont pleinement légitimes pour être motrices sur les sujets de la cybersécurité et de la résilience dans une optique de service à apporter aux acteurs de leurs territoires. Ce sont des personnes morales participant activement au fonctionnement de l'Association et se sont engagées à verser une cotisation pendant trois ans pour contribuer au fonctionnement de l'association et la réalisation de son objet, **elles sont des membres de droit**.
- les membres « **Institutions Publiques Locales Territoriales** » comprennent l'ensemble des établissements de coopération intercommunales ainsi que les institutions publiques locales avec une strate démographique de 40 000 habitants ou plus (Collectivités territoriales ou Etablissements Publics) participant activement au fonctionnement de l'Association et se sont engagées à verser une cotisation, pendant trois ans, pour contribuer au fonctionnement de l'association et la réalisation de son objet.

- les membres « **Institutions Publiques Locales** » qui sont des personnes morales participant activement au fonctionnement de l'Association et se sont engagées à verser une cotisation, pendant trois ans, pour contribuer au fonctionnement de l'association et la réalisation de son objet.
- les membres « **Institutions de l'Etat** » qui sont des Institutions représentant l'Etat et ses entités et services en matière de cybersécurité, de sûreté et de résilience, **elles sont des membres de droit**.
- les membres « **Entreprises** » qui sont des personnes morales participant activement au fonctionnement de l'Association et se sont engagées à verser une cotisation, pendant trois ans, pour participer au fonctionnement de l'association et la réalisation de son objet.
- les membres « **partenaires et bienfaiteurs** » qui sont des personnes morales soutenant financièrement l'association, et se sont engagés à s'acquitter une cotisation d'un montant supérieur à celui dû par les membres « actifs », ou, plus simplement, les personnes qui adressent régulièrement des dons à l'association.
- les membres « **honoraires** » qui sont des personnes morales ou physiques participants à la promotion des activités de l'Association.
- les membres « **qualifiés** » qui sont les personnes physiques et les personnes morales intéressées par les projets de l'Association et qui versent une cotisation annuelle d'un montant dont le minimum est fixé chaque année par l'assemblée générale ou qui ont été agréées spécialement par le conseil d'administration.

Pour faire partie de l'association, il faut être agréé par le bureau du conseil d'administration, qui statue sur les demandes d'admission présentées de l'association.

Le refus d'agrément n'a pas à être motivé.

ARTICLE 7. DROITS DES MEMBRES

Les catégories de membres de l'association disposent des droits suivants :

Catégorie	Nature juridique	Droit de vote AG
Membres « Collectivités Territoriales Chef de File »	Morale	Oui
Membres « Institutions Publiques Locales Territoriales »	Morale	Oui
Membres « Institutions Publiques Locales »	Morale	Oui
Membres « Institutionnels »	Morale	Oui
Membres « Entreprises »	Morale	Oui
Membres « Partenaires et bienfaiteurs »	Morale	Oui
Membres « Honoraires »	Morale ou physique	Non
Membres « Qualifiés »	Physique	Non

Tous les membres sont éligibles au conseil d'administration et sont destinataires des informations élaborées par l'Association.

Chaque membre s'oblige à respecter les présents statuts et le règlement intérieur de l'association.

ARTICLE 8. PERTE DE LA QUALITE DE MEMBRE

La qualité de Membre se perd par :

- le décès ou l'incapacité ;
- l'exclusion motivée et prononcée par le conseil d'administration, l'intéressé ayant été préalablement invité à présenter ses explications ;
- la démission notée au conseil d'administration par lettre recommandée avec accusé de réception ;
- le non-paiement de la cotisation pour les membres astreints à cette obligation de versement de la cotisation ;
- pour les personnes morales, la dissolution.

ARTICLE 9. CONSEIL D'ADMINISTRATION

9.1 Missions du conseil d'administration

Les pouvoirs de direction de l'association sont dévolus au conseil d'administration qui prend toutes décisions sous réserve de celles qui sont de la compétence d'un autre organe.

Le conseil d'administration détermine les axes stratégiques et les orientations de l'activité de l'association ainsi que les grands principes de fonctionnement de l'Association et veille à leur mise en œuvre.

Le conseil d'administration supervise le suivi des travaux et des publications de l'association et veille à leur diffusion.

Sur proposition du conseil d'orientation stratégique, le conseil d'administration est seul compétent pour procéder à la modification des présents statuts, à la transformation ou à la fusion de l'association. Le bureau tient informé l'Assemblée générale de l'ensemble des évolutions statutaire de l'Association.

Il peut se saisir de toute question intéressant la bonne marche de l'association et règle par ses délibérations les affaires qui la concernent.

Il autorise le président d'ester en justice au nom de l'association.

9.2 Composition du conseil d'administration

Le conseil d'administration est composé de cinq membres au moins et quinze au plus, dont les fondateurs de l'Association, les membres « Collectivités Territoriales Chef de File », et un collège d'administrateurs choisi désigné par les membres de l'assemblée générale disposant du droit de vote. Ils sont élus pour une durée de trois ans renouvelables dans les conditions suivantes :

Les membres du conseil d'administration qui sont des personnes physiques non-représentantes d'une personne morale sont nécessairement membres de l'association.

À tout moment, le conseil d'administration, sur proposition du président et dans la limite des places disponibles et le respect de la majorité des sièges détenus par les membres bienfaiteurs et les partenaires, peut coopter un nouveau membre siégeant au conseil d'administration. Cette cooptation doit être ratifiée lors de la prochaine assemblée générale dans les conditions prévues ci-dessus.

9.3 Fonctionnement du conseil d'administration

Les décisions du conseil d'administration sont prises à une majorité simple, chaque administrateur disposant d'une voix. En cas de partage, la voix du président est prépondérante.

Le conseil d'administration ne peut valablement délibérer que si cinq membres sont présents ou représentés. Un membre ne peut disposer que d'une seule procuration.

Les membres du conseil d'administration ne peuvent recevoir aucune rétribution à raison des fonctions qui leur sont confiées.

Le conseil d'administration peut élire un président d'honneur, disposant d'une voix consultative.

Les membres du conseil d'administration sont révocables par l'assemblée générale dans les conditions de l'article 16.

9.4 Bureau

La présidence de l'association est assurée à tour de rôle par chaque Collectivité Territoriale Chef de File pour une période de douze mois.

Le conseil d'administration choisit parmi ses membres un trésorier, un secrétaire et le cas échéant un ou deux vice-présidents, qui sont élus pour trois ans.

La fonction de trésorier peut être cumulée avec toute autre fonction que celle de président. La fonction de secrétaire peut être cumulée avec toutes les autres.

Le trésorier est responsable du contrôle des opérations financières importantes. Il est garant de la gestion comptable et tient les comptes de l'association. Il est chargé de l'appel des cotisations.

Enfin, il établit ou fait établir, sous sa responsabilité, les projets de comptes et de rapport de gestion annuels de l'association qui seront arrêtés par le conseil d'administration en vue d'une présentation et d'une approbation par l'assemblée générale.

Le secrétaire est chargé, en accord avec le président, des formalités administratives dues au fonctionnement des organes collégiaux de l'association (bureau, conseil d'administration, assemblée générale). Il établit ou fait établir les procès-verbaux de réunions du bureau, du conseil et de l'assemblée générale.

Il tient le registre prévu par l'article 5 de la loi du 1er juillet 1901.

Les fonctions de membres du bureau ne sont pas rémunérées mais ouvrent droit à remboursement des dépenses réalisées dans le cadre du mandat exercé.

ARTICLE 10. ATTRIBUTIONS DU PRESIDENT

Le président dispose des pouvoirs les plus étendus pour représenter l'association vis-à-vis des tiers.

Le président représente l'association en justice et dans tous les actes de la vie civile.

Il convoque le conseil d'administration.

Il préside les réunions du conseil d'administration et les assemblées générales.

Le président peut donner une délégation de pouvoirs spécifiques pour un ou plusieurs objets déterminés au directeur général.

ARTICLE 11. PERTE DE LA QUALITE DE MEMBRE DU CONSEIL D'ADMINISTRATION

Un membre du conseil d'administration perd sa qualité de membre du conseil d'administration en cas :

- de révocation ad nutum par l'assemblée générale ;
- de perte de sa qualité de membre d'association dans les conditions de l'article 8 ;
- de démissions du conseil d'administration ;
- pour un membre bienfaiteur ou un membre associé, de non-renouvellement de sa cotisation dans sa catégorie.

Il sera alors pourvu dans les conditions de l'article 9.2 à son remplacement lors de l'assemblée générale suivante. Toutefois, le conseil d'administration a la possibilité de coopter un membre dans les conditions de l'article 9.2 pour la durée restant à courir du mandat du membre sortant, ladite cooptation devant être ratifiée par la prochaine assemblée générale.

ARTICLE 12. REUNION DU CONSEIL D'ADMINISTRATION

Le conseil d'administration se réunit sur convocation du président, par lettre simple ou courrier électronique, aussi souvent que l'intérêt de l'association l'exige. Il peut également être convoqué, selon les mêmes modalités, par la moitié de ses membres. L'ordre du jour est fixé par le président.

Les réunions peuvent se tenir en distanciel.

Il est tenu procès-verbal des séances. Les procès-verbaux sont signés par le président et le secrétaire ou le trésorier. Les décisions ne sont exécutoires qu'après approbation du procès-verbal par le Conseil d'Administration.

À titre consultatif, le président peut inviter à la réunion du conseil d'administration toute personne utile à l'avancement des travaux de l'association.

ARTICLE 13. DIRECTEUR GENERAL

Sur proposition du président, le conseil d'administration désigne un Directeur Général chargé, sous le contrôle du président et du trésorier pour les attributions qui concernent ce dernier, d'assurer la gestion courante de l'association, dans le respect des principes définis par le conseil d'administration, les engagements de dépenses courantes et le suivi comptable relèvent de la compétence du président et du trésorier, qui peuvent en déléguer l'exécution au directeur général.

Le directeur peut être salarié de l'association.

Le directeur est membre du conseil d'administration et participe aux assemblées générales dans lesquelles il assiste le président, il ne dispose pas de droit de vote.

ARTICLE 14. CONSEIL D'ORIENTATION STRATEGIQUE

L'association est dotée d'un conseil d'orientation stratégique de cinq (5) membres au moins et de vingt (20) au plus. Le conseil d'orientation stratégique peut élire son propre président au sein des membres institutionnels et collectivités territoriales. Le président du conseil

d'administration et le directeur général assistent de droit aux réunions du conseil d'orientation stratégique.

Les membres du conseil d'orientation stratégique sont proposés par le président du conseil d'administration en concertation avec les membres « Collectivités Territoriales Chef de File », les membres « institutionnels » et les membres « collectivités territoriales » et sont ensuite désignés par le conseil d'administration, à la majorité des voix, pour une durée de trois ans.

Le conseil d'orientation stratégique se réunit autant que de besoin et a minima une fois par semestre physiquement ou par vidéoconférence. Le président de l'Association peut le réunir au moment où il apparaît nécessaire au Conseil d'administration de recueillir son avis sur les orientations opérationnelles ou stratégiques de l'Association.

ARTICLE 15. LES ASSEMBLEES GENERALES

L'assemblée générale ordinaire ne peut valablement délibérer que si le quart des membres bienfaiteurs, partenaires et associés est présent ou représenté.

En assemblée générale ordinaire, les décisions sont prises à la majorité simple des membres ayant le droit de vote présents ou représentés. En cas de partage, la voix du président est prépondérante.

L'assemblée générale extraordinaire ne peut valablement délibérer que si le tiers des membres bienfaiteurs, partenaires et associés est présent ou représenté. En cas d'absence de quorum, une nouvelle assemblée générale extraordinaire est convoquée dans un délai de quarante-huit heures ; elle pourra alors délibérer quel que soit le nombre de membres présents ou représentés.

En assemblée générale extraordinaire, les décisions sont prises à la majorité des deux tiers des membres ayant le droit de vote présents ou représentés.

Tout membre de l'association, à jour de ses cotisations, a le droit d'assister aux assemblées générales. Chaque membre bienfaiteur, partenaire ou associé a le droit de vote en assemblée générale et dispose d'une voix. Les membres qualifiés peuvent assister aux assemblées générales mais n'ont pas le droit de vote.

Les personnes morales participent aux assemblées par leurs représentants légaux ou par toute personne désignée à cet effet par ces derniers.

Les membres ayant le droit de vote qui ne peuvent être présents à l'assemblée générale peuvent donner pouvoir de les représenter à un autre membre ayant le droit de vote. Les membres ayant le droit de vote présents à l'assemblée générale ne peuvent détenir plus de cinq pouvoirs nominatifs. Les pouvoirs non nominatifs seront réputés établis en faveur des décisions proposées par le conseil d'administration.

Les membres ayant le droit de vote peuvent voter à distance par voie électronique en utilisant le formulaire prévu à cet effet et transmis avec l'avis de convocation. Le vote à distance par voie électronique sera pris en compte s'il est reçu par l'association, au plus tard aux dates et à l'heure indiquée dans l'avis de convocation, conformément aux indications données dans ledit avis de convocation. Un membre ne peut disposer de plus de trois (3) procurations.

Condition de modification des statuts

15.1 ASSEMBLEE GENERALE ORDINAIRE

Tous les membres peuvent assister à l'assemblée générale ordinaire dans les conditions de l'article 15. Elle se réunit au moins une fois par an, sur convocation du président, au lieu indiqué dans l'avis de convocation. Les convocations sont envoyées par lettre simple ou par courrier électronique, au moins quinze jours à l'avance ; elles doivent indiquer l'ordre du jour.

Le rapport annuel et les comptes sont adressés chaque année à tous les membres de l'association.

L'assemblée générale ordinaire entend le rapport de gestion du conseil d'administration, qui présente l'activité ainsi que les comptes de l'exercice arrêtés par le conseil d'administration. Elle approuve le rapport de gestion.

Elle délibère sur les questions inscrites à l'ordre du jour.

L'assemblée générale ordinaire désigne et révoque les membres du conseil d'administration et, le cas échéant, ratifie les cooptations de membres du conseil d'administration décidées par le conseil d'administration.

L'assemblée générale ordinaire, le cas échéant, désigné, révoque et fixe la rémunération du commissaire aux comptes de l'Association. Les administrateurs y compris le président sont révocables ad nutum étant précisé qu'ils pourront présenter leurs observations eu égard à cette révocation devant l'assemblée générale en respect du principe du contradictoire, sauf révocation décidée pour motif grave.

À titre consultatif, le président peut inviter à l'assemblée générale ordinaire toute personne utile à l'avancement des travaux de l'association.

Il est tenu procès-verbal des délibérations et des résolutions des assemblées générales. Les procès-verbaux de l'assemblée générale sont signés par le président et ils sont conservés dans un registre.

L'assemblée générale fixe le montant des *cotisation*s dans le règlement intérieur.

15.2 ASSEMBLEE GENERALE EXTRAORDINAIRE

Le président peut convoquer une assemblée générale extraordinaire, selon les mêmes modalités que celles prévues pour une assemblée générale ordinaire, le délai de convocation peut être réduit à 8 jours.

L'assemblée générale extraordinaire est également seule compétente pour se prononcer sur une dissolution de l'association, ainsi que sur ses modalités. En cas de dissolution, elle désigne un ou plusieurs commissaires chargés de la liquidation. En cas d'actif net, il est dévolu, selon les dispositions légales, à des établissements similaires.

ARTICLE 16. RESSOURCES

L'association ouvre un compte bancaire auprès de l'établissement financier de son choix et se donne tous pouvoirs pour accomplir également des actes de placement en fonction des opportunités de trésorerie. Les engagements de dépenses et le suivi comptable relèvent de la compétence du président et du trésorier, qui peuvent en déléguer l'exécution au directeur

général avec une limite de montant. La gestion bancaire et les relations avec le ou les organismes financiers relèvent de la compétence du président et du trésorier.

Les ressources de l'association proviennent :
- Des cotisations de ses membres ;
- Des subventions et des dons qu'elle est habilitée à recevoir ;
- Du produit de ses manifestations et de ses publications ;
- De toute autre ressource autorisée par la loi ;
- Des montants des cotisations ;
- Des dons ou les subventions ;
- Des ventes de produits dérivés résultant des activités menées par l'association ;
- De toutes les ressources autorisées par les lois et règlements en vigueur.

ARTICLE 17. REGLEMENT INTERIEUR

Le conseil d'administration prépare un règlement intérieur qui arrête les conditions d'exécution nécessaires des présents statuts. Il peut également préciser divers points non prévus par les statuts. Le règlement intérieur est adopté et modifié, le cas échéant, par l'assemblée générale ordinaire.

ARTICLE 18. FORMALITES

Le président est chargé, avec faculté de délégation, de remplir toutes les formalités de déclaration et de publication prescrites par la réglementation.

Tous pouvoirs sont également donnés au porteur des présents à l'effet d'effectuer les formalités.

Fait à Basse-Terre, le 12 juillet 2022, en 5 exemplaires.

Signature des membres du bureau

Madame Aurélie BITUFWILA
Président de l'association « ACCYB »
Conseil régional de Guadeloupe

Monsieur Charles-Adolphe ROULLET
Secrétaire de l'association « ACCYB »
Groupe LORET (AGI)