SOLURIS
SOLUTIONS NUMÉRIQUES TERRITORIALES INNOVANTES

DÉLIBERATION
BUREAU SYNDICAL
Réunion du 1er juin 2023

Date de la convocation : 25 mai 2023
Nombre de membres en exercice : 17
Nombre de membres présents/votants : 12
Nombre de pouvoirs : 3
Nombre de membres absents ou excusés : 5

L'an deux mil vingt-trois, le premier juin à dix heures vingt, le Bureau Syndical s'est réuni à Saintes, sous la Présidence de Madame Céline VIOLLET qui ouvre valablement la séance, le quorum étant atteint.

Étaient présents : Serge BERNET, Sabine BESIAT, Hubert COUPEZ, Jean-Michel MARCHAIS, Jean-Pierre MORDANT, Monique RIVIÈRE, Agnès RONDEAU, Romain ROUAN, Céline VIOLLET.

1 pouvoir de Jacky BOTTON à Céline VIOLLET

1 pouvoir de Jean-Pierre LE CLOEREC à Hubert COUPEZ

1 pouvoir de Raymond MOHSEN à Jean-Pierre MORDANT

Étaient absents ou excusés : Mariette ADOLPHE Jacky BOTTON Vincent COPPOLANI, Emmanuel ECALE, Patrick GUYOT, Jean-Pierre LE CLOËREC, Raymond MOHSEN, Marie NEDELLEC.

Assistaient également à la réunion : Benoît LIÉNARD, Nathalie BACQUET, Diane GERMAIN, Antoine MALETRAS, Véronique VERNOUX et Claire ZONCA.

Secrétaire de séance : Jean-Pierre MORDANT.

CONTRAT

202336 Convention de collaboration avec le campus régional de cybersécurité et de confiance numérique de Nouvelle Aquitaine

Vu les articles L 5721-1 et suivants du Code Général des Collectivités Territoriales,

Vu la loi du 1er juillet 1901 relative au contrat d'association,

Vu les statuts du Syndicat Soluris,

Considérant que la confiance numérique et la cybersécurité sont des axes majeurs du développement des services de SOLURIS ,

Il est proposé de signer une convention de coopération avec le Campus Cybersécurité de Nouvelle Aquitaine

En effet, l'action de Soluris en matière de confiance numérique s'étend également au niveau national par la participation à de nombreuses instances où la compétence de Soluris est reconnue par les autorités nationales (ANSSI, CNIL, GIP Cybermalveillance.gouv.fr, …) comme par les associations de collectivités locales (AMF, Déclic, FNCCR, …).

En Nouvelle-Aquitaine, Soluris participe depuis 2018 à différents réseaux d'échanges sur la cybersécurité, dans le cadre d'événements (ex. colloque « Charente-Maritime

CyberSécurité », réunions de l'Institut des Hautes Etudes de la Défense Nationale, etc.) ; depuis 2019, aux réunions de préfiguration du « Centre de Ressources Cybersécurité Nord Nouvelle-Aquitaine » situé à Niort et y représente le secteur des collectivités locales, aux côtés des représentants d'autres secteurs (économie, recherche, etc.).

Parallèlement le Conseil régional de Nouvelle-Aquitaine a adopté en juillet 2020 une feuille de route en matière de cybersécurité, dont la création d'un campus régional dédié à la cybersécurité (ou Campus Cyber NA) constitue le pilier central. Il permettra la mise en cohérence de toutes les actions présentes et à venir et la mise en réseau des centres de ressources en cyber sécurité (CRC) territoriaux déjà initiés, suivant les recommandations de la Revue stratégique de cyberdéfense de février 2018[1]. En fédérant les talents et les acteurs de la filière cybersécurité autour de projets innovants et collaboratifs, le Campus Cyber NA sera la vitrine à l'international de l'écosystème néo-aquitain en cybersécurité. Il aura pour vocation d'accélérer la mise en œuvre des ambitions régionales en matière de cybersécurité.

Une première brique opérationnelle est développée, qui apporte un premier service aux entreprises et collectivités du territoire en prenant en charge la création et la mise en œuvre d'un centre de réponse aux attaques informatiques (CSIRT - Computer Security Incident Response Team). Ce service permettra la consolidation et la qualification des incidents dont il aura été saisi et la mise en relation de l'entité victime avec les organisations en charge de l'accompagner dans la résolution de l'incident (prestataires de solutions de sécurité informatique et services de police et gendarmerie). »

Le Campus Cybersécurité de Nouvelle Aquitaine a également vocation à déployer sur l'ensemble du territoire régional un ensemble de diagnostics (maturité cyber, relevé de vulnérabilités, recherche de compromission) à destination de ses bénéficiaires (entreprises, collectivités, établissements publics locaux et associations), permettant l'élaboration d'un observatoire régional de l'exposition des organisations aux cybermenaces.
La Région Nouvelle-Aquitaine bénéficiant d'un maillage dense d'opérateurs de services numériques (OPSN), œuvrant au bénéfice des collectivités et notamment des plus petites d'entre elles et se trouvant de fait au premier rang des interlocuteurs de confiance naturels sur les sujets de cybersécurité. De par leur nature et le rôle qu'ils exercent au bénéfice des collectivités adhérentes, les OPSN du territoire néo-aquitain ont vocation à exercer un rôle particulier au sein du Campus Cybersécurité de Nouvelle Aquitaine et des centres de ressources locaux associés.

Le projet de convention est joint en annexe de la présente fiche.
Les crédits nécessaires sont inscrits au budget.

1 Revue stratégique de cyberdéfense, SGDSN, 12 février 2018.

Après en avoir délibéré, les élus du Bureau Syndical autorisent, à l'unanimité, la Présidente à

- *Collaborer étroitement avec les acteurs du Campus en cas d'incident cyber touchant les collectivités adhérentes à Soluris,*
- *Partager des informations et de la veille,*
- *Mener des actions conjointes de montées en compétences, formations et entrainement (à la gestion de crise notamment),*
- *D'approuver la convention (en annexe),*
- *D'autoriser la Présidente à signer cette convention ainsi que toutes les pièces et documents nécessaires à la mise en œuvre de cette mission.*

Nombre de voix POUR : 12
Nombre de voix CONTRE : 0
Abstentions : 0

Pour copie conforme,
Le secrétaire de séance,
Jean-Pierre MORDANT

La Présidente,
Céline VIOLLET.

CONVENTION DE COOPÉRATION

ENTRE

LE CAMPUS RÉGIONAL DE CYBERSECURITE ET DE CONFIANCE NUMÉRIQUE

ET

L'OPSN « XXX »

~~

ENTRE

L'OPSN « XXX »
ci-après dénommée « XXX » d'une part ;

ET

Le Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine, association loi 1901, sise au 6, allée du Doyen Georges Brus à Pessac, représentée par Mathieu HAZOUARD, en qualité de Président,

ci-après dénommée « **Campus Cyber NA** » d'autre part ;

PRÉAMBULE

Dans la lignée de la stratégie européenne de cybersécurité adoptée en décembre 2020 par la Commission européenne, la stratégie française de cybersécurité a été annoncée le 18 février 2021 par le Président de la République française. Son objectif est de garantir la maîtrise des technologies critiques en matière de cybersécurité par des acteurs français de confiance, et d'accélérer le développement de ce secteur économique, afin d'assurer et de renforcer de façon pérenne la sécurité des citoyens, des entreprises, des administrations et de l'ensemble des acteurs économiques. De plus, dans le cadre du plan de relance, l'Etat prévoit un volet cybersécurité piloté par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Si ce volet vise à profiter au plus grand nombre d'acteurs publics, une importance particulière est accordée aux collectivités territoriales et aux organismes au service du citoyen. Ainsi, des subventions sont proposées aux régions afin de favoriser la création d'équipes de proximité destinées à assister le tissu économique et social local.

Le Conseil régional de Nouvelle-Aquitaine a, pour sa part, très tôt affiché son ambition de faire de la Nouvelle-Aquitaine un territoire de confiance numérique : cet engagement s'est traduit par l'adoption en juillet 2020 d'une feuille de route en matière de cybersécurité. Le fil conducteur ayant conduit à l'élaboration et la mise en œuvre de la feuille de route régionale de cybersécurité pourrait se résumer ainsi : « Pas de cybersécurité sans un climat de confiance, et pas de confiance numérique sans relations de proximité, entre les citoyens, les entreprises, les administrations et autres acteurs socio-économiques de la Nouvelle-Aquitaine ».

La création d'un campus régional dédié à la cybersécurité constitue le pilier central de l'ambition régionale en matière de cybersécurité et de confiance numérique et correspond à l'action 1 de la feuille de route. Il permettra la mise en cohérence de toutes les actions présentes et à venir et la mise en réseau des centres de ressources en cyber sécurité (CRC) territoriaux déjà initiés, suivant les recommandations de la Revue stratégique de cyberdéfense de février 2018[1]. En fédérant les talents et les acteurs de la filière cybersécurité autour de projets innovants et collaboratifs, le Campus

1 Revue stratégique de cyberdéfense, SGDSN, 12 février 2018.

Cyber NA sera la vitrine à l'international de l'écosystème néo-aquitain en cybersécurité. Il aura pour vocation d'accélérer la mise en œuvre des ambitions régionales en matière de cybersécurité.

Pour assurer la pertinence de cette initiative et son ancrage fort dans le territoire, une première brique opérationnelle est développée, qui apporte un premier service aux entreprises et collectivités du territoire en prenant en charge la création et la mise en œuvre d'un **centre de réponse aux attaques informatiques (CSIRT - *Computer Security Incident Response Team*)**. Ce service permettra la consolidation et la qualification des incidents dont il aura été saisi et la mise en relation de l'entité victime avec les organisations en charge de l'accompagner dans la résolution de l'incident (prestataires de solutions de sécurité informatique et services de police et gendarmerie).

Par la suite, le Campus cyber NA pourra s'appuyer sur la connaissance de l'incidentologie régionale pour alimenter les formations proposées en son sein et s'assurer de la pertinence des projets d'innovations qu'il portera. Cette connaissance a vocation à être diffusée au sein de la filière régionale des entreprises cyber et à alimenter les centres territoriaux de ressources et les services de l'Etat, pour lesquels une connaissance précise de l'état de la menace est nécessaire.

Le positionnement territorial très fort du Campus et renforcé par ses relations opérationnelles avec des acteurs européens lui permettra également d'entraîner la communauté des entreprises néo-aquitaines dans des projets européens de grande envergure, nécessitant la plupart du temps la formation de consortium transnationaux.

Le Campus cyber NA a également pour vocation de déployer sur l'ensemble du territoire régional un ensemble de diagnostics (maturité cyber, relevé de vulnérabilités, recherche de compromission) à destination de ses bénéficiaires (entreprises, collectivités, établissements publics locaux et associations), permettant l'élaboration d'un observatoire régional de l'exposition des organisations aux cybermenaces.

Par ailleurs, la région Nouvelle-Aquitaine bénéficie d'un maillage dense d'opérateurs de services numériques (OPSN), œuvrant au bénéfice des collectivités et notamment des plus petites d'entre elles et se trouvant de fait au premier rang des interlocuteurs de confiance naturels sur les sujets de cybersécurité. De part leur nature et le rôle qu'ils exercent au bénéfice des collectivités adhérentes, les OPSN du territoire néo-aquitain ont vocation à exercer un rôle particulier au sein du Campus Cyber NA et des centres de ressources locaux associés, que la présente convention encadre.

[à compléter]

EN CONSÉQUENCE DE QUOI IL A ÉTÉ CONVENU CE QUI SUIT :

Article 1

Objet de la Convention

Le Campus cyber NA et « XXX » conviennent qu'il est de leur intérêt mutuel de coopérer en matière de cybersécurité, de confiance numérique et lutte contre la cybercriminalité. L'objectif majeur de cette coopération est de contribuer ensemble à accroître la sécurité numérique du territoire régional, par des actions concertées, un partage d'expérience et une montée en compétences mutuelle des Parties.

Cette coopération prend principalement la forme d'échange d'information entre les services de « XXX » et le Campus cyber NA, d'appui mutuel en matière de formation et de sensibilisation, de réponse et d'anticipation des incidents et de renforcement des pratiques de cybersécurités dans les collectivités, sans que ces domaines soient exhaustifs.

La présente Convention a pour objet de définir les modalités et les conditions par lesquelles « XXX » et le Campus Cyber NA s'accordent sur le principe de cette coopération et les mettent en œuvre au sein du Centre de ressources en cybersécurité auquel est rattaché le territoire couvert par « XXX ».

Article 2

Mise en œuvre du dispositif

Article 2.1. Interconnexion entre les parties

Les Parties prenantes se transmettent mutuellement, en annexe à la présente, l'identité et/ou la fonction, ainsi que les coordonnées téléphoniques et adresses de courrier électronique des points de contacts privilégiés de chacune des Parties chargés de réaliser les actions de coopération.

Chaque Partie notifiera à l'autre tout changement de coordonnées de ces points de contact.

Article 2.2. Schéma du dispositif

En tant que de besoin, les Parties s'engagent à répondre au mieux aux sollicitations entrant dans le cadre de la présente. A cet effet, un lien direct peut être établi entre les Parties dans les domaines qui relèvent de leurs compétences respectives.

La nature des faits justifiant l'activation de ce lien direct sera précisée par le Parties au fur et à mesure de la présente collaboration, notamment lors des réunions de coordination tenues selon les modalités de l'article 4 des présentes.

Article 2.3. Centre de ressources cyber

Dans le cadre de la déclinaison territoriale de son action, le Campus cyber NA facilite l'émergence et le fonctionnement de Centre de ressources en cybersécurité (CRC), au plus proche des besoins des territoires. Ces CRC ont pour vocation de décliner localement les missions et objectifs du Campus cyber NA, dont ils bénéficient des ressources produites (outils, services et contenus pédagogiques).

Au titre de son rôle et de ses missions auprès de ses adhérents, « XXX » exercera le rôle de CRC pour les collectivités du territoire concerné.

Article 2.4. Échanges d'informations

Échanges d'informations générales :

Dans le cadre de la veille générale (sources ouvertes, retour d'expérience, partenariats, analyses de phénomènes…), les parties peuvent échanger mutuellement leurs connaissances dans le domaine de la cybersécurité et de la cybercriminalité, de manière générale ou directement en lien avec le territoire.

Dans le cadre de la mise en œuvre des outils de diagnostics fournis par le Campus cyber NA, « XXX » s'engage à lui en remettre les résultats à des fins d'alimentation de l'observatoire régional et de connaissance des territoires. En retour, le Campus cyber NA s'engage à transmettre à « XXX » toute donnée statistique consolidée concernant son territoire.

Ils pourront également partager des informations sur les expérimentations, les projets de recherche et de développement, les modifications réglementaires et législatives aux fins d'une meilleure connaissance de l'environnement de la cybersécurité, que ce soit au niveau régional, national ou européen.

Échanges d'information lors d'un incident :

De manière générale, le Campus Cyber NA peut être détenteur d'informations relatives à des attaques informatiques susceptibles d'avoir un impact important sur la sécurité collective et les services rendus au public, soit en raison de leur fréquence, soit en raison du territoire ou du secteur d'activité concerné. A ce titre, le Campus Cyber NA peut solliciter les conseils des services de « XXX », dans le respect du cadre juridique actuellement en vigueur, et notamment le Règlement général sur la protection des données (RGPD), et transmet les informations utiles à la maîtrise de la menace et la protection des victimes.

Le premier contact avec la collectivité victime d'une attaque cyber, qu'il soit établi auprès du Campus cyber NA ou auprès de « XXX », permettra de diffuser les conseils d'urgence quant aux mesures nécessaires pour la préservation de la preuve numérique, et une première sensibilisation sur l'éventuelle judiciarisation de sa déclaration, si elle le souhaite, dans le cadre d'un dépôt de plainte.

Le Campus cyber NA demandera systématiquement à la collectivité victime son consentement, en préalable à la transmission de l'intégralité des informations aux services de « XXX ». En cas de refus, les informations personnelles transmises seront pseudonymisées afin de permettre leur transmission d'une part, et une levée ultérieure de l'anonymat en cas de changement d'avis.

Réciproquement, lorsqu'un acte de cyber-malveillance est déclaré à « XXX », la victime est orientée vers les interlocuteurs du Campus Cyber NA, pour coordonner l'accompagnement et l'accès aux acteurs de la remédiation, prestataires labellisés au plan national par l'ANSSI et Cybermalveillance.

Article 2.5. Appui mutuel en matière de formation

Aux fins de poursuivre la montée en compétence mutuelle des deux parties, il est convenu que les parties s'apportent un appui en matière de formation. Cet appui peut prendre la forme d'invitations des spécialistes de « XXX » à intervenir lors de formations spécifiques. Parallèlement, le Campus Cyber NA peut proposer des formations permettant de consolider les connaissances et compétences desdits spécialistes.

Dès lors que les services de « XXX » sont sollicités par une collectivité relevant de la zone d'intervention du Centre de ressources cyber du territoire pour des avis relatifs à la cybersécurité, ils ont la liberté de se mettre en relation avec le Campus Cyber NA, afin que ce dernier puisse apporter la réponse la plus adaptée en termes de formation ou de sensibilisation.

Article 2.6. Campagne de recherche de compromission et de réduction de vulnérabilités

Périodiquement, le Campus cyber NA peut adresser à « XXX » des outils et indicateurs permettant de mener des campagnes de recherche de compromission. « XXX » s'engage à mettre en œuvre, dans la mesure de ses moyens, cette recherche auprès des collectivités de son territoire et à en faire connaître les résultats au Campus cyber NA, qui communiquera en retour les mesures à mettre en œuvre afin de pallier à l'infection découverte.

Dans le cadre de son activité de réponse à incidents, le Campus cyber NA peut découvrir l'existence de vulnérabilités partagées par les collectivités du territoire. Il communiquera dans ce cas, selon des moyens adaptés à la sensibilité de l'information, à « XXX » la nature et la gravité de la vulnérabilité détectée, ainsi que les procédures de correction. « XXX » s'engage à transmettre l'information aux collectivités concernées et à les accompagner dans la mise en œuvre des procédures de protection.

Article 2.7. Entraînement et exercices

Dans le cadre de l'organisation et la conduite d'exercice de gestion de crise cyber, le Campus Cyber NA peut, en tant qu'organisateur ou contributeur, proposer, sans engagement de leur part, la participation des services « XXX », selon des modalités cohérentes avec le niveau et les objectifs de ces exercices (observation, conseil, participation active…). Réciproquement, « XXX » peut proposer de faire participer le Campus cyber NA aux exercices de gestion de crise mis en œuvre sur le territoire du CRC concerné.

Article 2.8. Crise majeure

Dans le cadre de la gestion d'une crise majeure d'origine cyber touchant les collectivités du territoire concerné, les équipes du Campus cyber NA pourront être associés à la coordination de l'action régionale en lien avec l'ANSSI, Agence nationale de sécurité des systèmes d'informations et rendront compte à la Préfecture de région.

Article 3

Dispositions financières

La présente convention est établie à titre gratuit, dans la mesure où elle ne fait que préciser les conditions particulières de mise en œuvre du rôle de chacun, acquit dans le cadre de l'adhésion régulière de « XXX » au Campus cyber NA. Chacune des parties supporte par ailleurs ses propres coûts qui pourraient éventuellement naître de l'exécution de la présente convention.

Article 4

Pilotage et évaluation de la coopération

Les parties pourront échanger en tant que de besoin de manière collaborative afin d'identifier et de discriminer de manière objective l'ensemble des difficultés rencontrées par chacune d'entre elles dans l'exécution de la présente convention.

Cette convention donnera lieu à une réunion annuelle dans l'objectif de réaliser un bilan et de dresser les perspectives de la coopération entre les Parties. Une réunion de coordination sera également organisée chaque semestre afin d'examiner les éventuelles difficultés et/ou bonnes pratiques de la coopération entre les Parties, et de proposer les ajustements nécessaires.. Lors de cette réunion de coordination semestrielle, les Parties pourront inviter à participer des intervenants représentant les membres de l'association du Campus Cyber NA et les services de l'Etat compétents en matière de cyberséscurité.

Article 5

Confidentialité et communication

Les informations recueillies par le Campus Cyber NA auprès des victimes ou d'autres parties, peuvent présenter un caractère sensible qui nécessite la mise en place de mesures spécifiques de protection et une attention particulière lors des traitements effectués.

Certaines informations échangées dans le cadre de la présente Convention peuvent recouvrir un caractère confidentiel et seront appelées « Informations Confidentielles » ci-après. Sans que l'énumération ci-après ne soit limitative :

(i) toute information écrite ou verbale quel qu'en soit le support, la forme ou la nature, concernant notamment ou des éléments relatifs aux marchés, clients, accords, actifs, procédures, marketing ou de nature technique, opérationnelle, industrielle, environnementale, scientifique, administrative, comptable, commerciale, économique, concurrentielle, sociale, managériale, organisationnelle, financière, fiscale, juridique et judiciaire, et relative directement ou indirectement à une Partie et/ou ses sociétés affiliées/unités dont l'autre Partie aurait connaissance dans le cadre de la présente Convention ;

(ii) les travaux, études, rapports, synthèses, expertises, avis, opinions, correspondances, organigrammes, listes, savoir-faire ou tous autres documents de quelque forme, nature ou provenance que ce soit, qui font référence ou résultent des Informations Confidentielles définies au paragraphe (i) ci-dessus.

Chaque Partie s'engage à tenir confidentielles les informations qu'elle recevra des autres Parties et/ou de ses sociétés affiliées/unités, et services de l'Etat consultés, et notamment à ne pas divulguer ces informations à un tiers quelconque, autre que ses employés ou intervenants ayant besoin de les connaître, et de ne les utiliser qu'à l'effet d'exercer ses droits et de remplir ses obligations aux termes de la présente Convention.

Nonobstant ce qui précède, l'obligation de confidentialité susvisée ne s'appliquera pas aux informations qui :

(i) seraient tombées ou tomberaient dans le domaine public indépendamment de la faute de la Partie les ayant reçues ;

(ii) seraient développées à titre indépendant par la Partie destinataire ;

(iii) seraient connues par la Partie destinataire avant que la Partie divulgatrice ne les lui communique ;

(iv) seraient légitimement reçues d'un tiers non soumis à une obligation de confidentialité ;

(v) seraient légitimement portées à la connaissance de la Partie destinataire en l'absence d'une obligation de confidentialité ou d'un manquement à la présente Convention ;

(vi) devraient être divulguées en vertu de la loi ou sur ordre d'une autorité publique, auquel cas elles ne devront être divulguées que dans la mesure requise et après en avoir prévenu par écrit l'autre Partie.

Les obligations des Parties à l'égard des Informations Confidentielles demeureront en vigueur pendant toute la durée de la Convention et pendant une période de cinq (5) ans après son expiration ou résiliation.

La Partie destinataire devra restituer toutes les copies des documents et supports contenant des Informations Confidentielles, dès la fin de la Convention, quelle qu'en soit la cause.

Chaque Partie s'engage à faire respecter les obligations au titre de la présente Convention par son personnel, ses intervenants ou tiers qui pourraient intervenir à quelque titre que ce soit dans le cadre de la Convention.

Chaque Partie reconnaît que seuls les employés, sociétés affiliées et contractants ayant besoin de connaître les Informations Confidentielles y auront accès, sous réserve que ces personnes aient accepté par écrit de respecter des obligations de confidentialité au moins équivalentes à celles exposées dans la présente Convention.

Si une Partie divulgue ou utilise des Informations Confidentielles en violation de la présente Convention, l'autre Partie pourra, nonobstant tout autre recours dont elle bénéficie, solliciter des mesures conservatoires afin d'interdire ces actions.

Aucune Partie ne pourra faire mention ou usage du nom, de la dénomination, des marques et logos ou autres appellations, commerciales ou non, de l'autre Partie, sans accord préalable et écrit de cette dernière. Les Parties reconnaissent que la remise du logo de l'autre Partie ne lui confère aucun droit de propriété sur ce logo et tout élément d'identification.

Pendant la durée de la présente Convention, chacune des Parties est autorisée à communiquer sur la présente Convention ainsi que sur les actions entreprises dans le cadre de la présente Convention .

Article 6

Traitement des données à caractère personnel

Afin d'assurer le respect du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre de circulation de ces données (« RGPD »), les Parties s'engagent à respecter les dispositions applicables en matière de données personnelles dans le cadre de l'exécution de la présente Convention. Dans le cadre de l'exécution de cette Convention, chaque Partie doit être qualifiée de responsable de traitement indépendant de l'autre Partie. A ce titre, chaque Partie s'engage à traiter les données personnelles en conformité avec le RGPD et autres législations applicables, notamment en assurant la protection des droits des personnes concernées, en garantissant la sécurité et la confidentialité des données personnelles traitées, notamment par la mise en place de mesures internes organisationnelles et de sécurité et en assurant la licéité du traitement. En tant que responsable de traitement indépendant, chaque Partie restera intégralement et individuellement responsable des traitements des données personnelles qu'elle entreprend en vertu de cette Convention, et en particulier à l'égard de toute demande d'indemnisation introduite par une personne qui a subi un préjudice matériel ou moral du fait d'une violation de la réglementation applicable. Dans l'hypothèse où une Partie serait amenée à traiter des Données Personnelles pour le compte de l'autre Partie dans le cadre de la présente Convention, elle l'en informera promptement. A cet égard, les Parties s'approcheront en vue de compléter la présente Convention afin que les traitements des données personnelles réalisés dans le cadre de la Convention demeurent conformes à la réglementation en vigueur.

Article 7

Responsabilité — Assurances

Chaque Partie à la Convention est responsable (a) des actions et omissions propres à son activité effectuées sous son contrôle et (b) du non-respect de la Convention.

En conséquence, chaque Partie est tenue de réparer, selon les règles de droit commun, les dommages causés à l'autre Partie et aux tiers qui lui sont imputables.

Dans l'hypothèse où les intervenants d'une Partie seraient amenés à se rendre dans les locaux de l'autre Partie, cette Partie se porte forte du respect par ses intervenants des règles en matière d'hygiène et de sécurité et le règlement intérieur applicables dans lesdits locaux.

Article 8

Résiliation de la Convention — Cas de force majeure

Chaque Partie pourra résilier la Convention en cas de manquement aux obligations contractuelles de l'autre Partie, sous réserve d'une mise en demeure préalable restée infructueuse pendant une durée de dix (10) jours.

Aucune des Parties ne sera responsable, ni ne sera considérée comme n'ayant pas respecté les dispositions de la présente Convention, en cas de défaut d'exécution de ses obligations issues de la présente Convention dû à un événement de force majeure, tel que ce terme est défini à l'art. 1218 du code civil. Dans une telle hypothèse, les Parties conviennent de se rencontrer et de faire leur possible pour minimiser les conséquences de l'événement de la force majeure. Dès que l'empêchement dû à la force majeure cesserait, la Partie affectée par un événement de force majeure reprendra l'exécution de ses obligations pour le reste du terme de la Convention.

Article 9

Droit applicable et litiges

La présente Convention est régie par le droit français.

En cas de litige relatif à l'interprétation ou à l'exécution de la présente Convention, les Parties s'obligent à se rapprocher afin de parvenir à sa résolution amiable. Au cas où les Parties ne parviendraient pas à trouver une solution amiable dans un délai de trente (30) jours, tout litige pouvant survenir à l'occasion de l'interprétation et/ou de l'exécution de la présente Convention devra être soumis aux tribunaux compétents.

Article 10

Durée de la Convention — Avenants — Intégralité de l'accord

La présente Convention entre en vigueur le jour de sa signature et est conclue pour une durée initiale de cinq (« 5 ») ans, renouvelable par tacite reconduction.

Dans le cadre des réunions de coordination, les Parties peuvent proposer des modifications de la présente Convention.

Toute modification de l'une ou l'autre des clauses de la présente Convention (hors annexe I) devra faire l'objet d'un avenant écrit signé par les représentants dûment autorisés des Parties.

La présente Convention exprime l'intégralité de l'accord intervenu entre les Parties. Elle annule et remplace tout accord ou contrat passé antérieurement, et tout autre acte de toute nature échangé à ce propos, qu'il ait été simplement soumis à l'attention de l'autre Partie ou signé par les deux Parties.

La présente Convention contient 8 feuillets auxquels s'ajoutent deux annexes. Elle est établie en deux exemplaires, signés par les Parties.

Fait à YYYY, le XXX

ANNEXE

LISTE DES CORRESPONDANTS

Campus Cyber NA

Contact convention :

Guy FLAMENT, Directeur,
directeur@campuscyber-na.fr, +33 6 63 05 31 48

Philippe STEUER, responsable du CSIRT,
philippe.steuer@campuscyber-na.fr, +33 7 55 59 19 16

Contact signalement d'incident :

Contact opérationnel CSIRT : incident@campuscyber-na.fr 0805 29 29 40