**CONVENTION D’ACCOMPAGNEMENT**

**A LA CYBERSECURITE**

ENTRE

[NOM collectivité]

dont le nº SIREN est

et dont le siège est sis

ci-après désigné la « COLLECTIVITE »,

représenté (e) par , dûment habilité à signer les présentes

d'une part,

ET

**« Le Syndicat Mixte Mégalis Bretagne** »

dont le n° SIRET est 25351449100047

et dont le siège est 15 Rue Claude Chappe, 35510 Cesson-Sévigné,

ci-après désigné MEGALIS,

représenté par son Président, Monsieur Loïg CHESNAIS-GIRARD, dûment habilité à signer les présentes

Il est convenu ce qui suit :

PREAMBULE

Par délibération du 15 décembre 2021, le Syndicat mixte Mégalis Bretagne a validé la création d’une offre d’accompagnement à la cybersécurité.

Le Syndicat mixte Mégalis Bretagne a défini un cadre de prestations en matière de cybersécurité avec le Groupement d’Intérêt Public SIB, domicilié à Rennes.

Le présent document présente les modalités d’actions, les responsabilités et les engagements entre MEGALIS BRETAGNE et la COLLECTIVITE bénéficiaire du service. Dans ce cadre le GIP SIB agit pour le seul compte du Syndicat Mixte Mégalis Bretagne en tant qu’opérateur technique desdites prestations.

L’accompagnement à la cybersécurité comprend deux parcours :

* Parcours 1 | Cyber Sensibilisation
	+ Accompagnement de sensibilisation, formation à destination de toutes les collectivités ;
	+ La réalisation d’une campagne phishing
* Parcours 2 | Cyber Sensibilisation enrichi à destination :
	+ des communes < 3500 habitants
	+ des EPCI < 20 000 habitants ;

En complément des actions du parcours cyber sensibilisation, ce parcours intègre :

* Un pré-audit du système d’information (état des lieux de l’administration des serveurs internes, la gestion des postes de travail, la gestion des sauvegardes, et les serveurs externes)
* Des actions techniques de tests de vulnérabilité opérationnelles. A ce titre, celles-ci nécessitent le déploiement de matériel au sein du Système d’Information de la COLLECTIVITE.

Les prestations porteront uniquement sur les équipements, services et données utilisés par la COLLECTIVITE d’un parcours d’accompagnement, à l'exclusion de tout autre entité.

# OBJET DE L’ACCOMPAGNEMENT

Le parcours d’accompagnement à la cybersécurité vise à élever le niveau de maturité global de la COLLECTIVITE (agent, élu et Système d’Information), et autant que faire ce peut définir des pistes d’améliorations, voire la préconisation des conditions de leurs mises en œuvre.

# Cadrage des actions realisees

Les périmètres des actions définies conjointement entre le Syndicat mixte Mégalis Bretagne et la COLLECTIVITE sont énoncés par nature de parcours.

Sur demande les prestations de services des parcours MEGALIS sont interchangeables. Dans ce cas, l’avis de l’opérateur technique sera requis pour des questions technico-organisationnelles.

## Parcours 1 | Cyber Sensibilisation

Pour le parcours d’actions de sensibilisation**,** MEGALIS propose à la COLLECTIVITE :

* Un ensemble de contenus de sensibilisation,
* Une intervention en présentiel ou à distance dans le cadre d’instance (conseil ou commission),
* L’organisation d’une réunion de présentation à destination des agents, en présentiel ou à distance,
* L’accès à des webinaires,
* La réalisation d’une campagne phishing
* Un accès pendant la durée du parcours à un module de e-learning
	+ Le choix est laissé à la collectivité de recourir ou non à ce module pour ses agents, élus. Dans le cas du choix d’accès au module, Mégalis fournira à l’opérateur technique la liste des adresses mails des personnes concernées pour implémentation.

Le parcours sera encadré par une réunion de lancement et une réunion de restitution. Cette dernière sera l’occasion de restituer les livrables afférents aux actions réalisées.

MEGALIS et la COLLECTIVITE définiront d’un commun accord les modalités pratiques de ce parcours.

Les campagnes de phishing seront réalisées parl’opérateur technique pour le compte de MEGALIS selon des scénarios prédéfinis.

Le phishing (ou hameçonnage en français) est une technique frauduleuse destinée à leurrer l’internaute pour l’inciter à communiquer des données personnelles (comptes d’accès, mots de passe, donnée bancaire…) en se faisant passer pour un tiers de confiance.

L’opérateur technique affectera les moyens techniques et humains nécessaires à la bonne organisation et réalisation de la campagne de phishing.

La cible de la campagne est la suivante :

* L’ensemble des agents et élus de la collectivité requérante.

Mégalis s’assurera auprès de son opérateur technique de la seule collecte des données uniquement essentielles à l’exécution et analyse de la campagne. A ce titre les données collectées sont :

* L’adresse email,
* L’heure d’ouverture,
* L’heure du clic,
* L’heure de soumission de données

L’opérateur technique fournira à la fin de la campagne de phishing une compilation des résultats dans un livrable explicatif. A l’issue de la campagne, l’ensemble des données collectées sont supprimées.

## parcours 2 | Cyber Sensibilisation enrichi

Au titre de ce parcours, Mégalis propose un pré-audit du système d’information à la COLLECTIVITE afin de l’accompagner à la réalisation d’un état des lieux de son Système d’Information sur les thématiques suivantes :

* Administration des serveurs internes,
* Gestion des postes de travail,
* Gestion des sauvegardes et serveurs externes.

Les modalités de ce pré-audit sont :

* Remplir une fiche d’identité de la collectivité et de ses prestataires afin de dessiner le périmètre à sécuriser,
* Remplir ou faire remplir par le(s) prestataire(s) un questionnaire. Ce questionnaire dit « prestataire » doit permettre de connaître le niveau de sécurité des prestataires intervenant sur le Système d’Information de la collectivité. Ce questionnaire pourra être réutilisé par la COLLECTIVITE comme standard de sécurité lors de la constitution de prochains marchés publics.
* Remplir un questionnaire dit « sécurité des services », celui-ci aidera à évaluer la sécurité générale du Système d’Information. Ce questionnaire n’est pas nécessairement un caractère exhaustif, toutefois il balaiera les points clefs du système informatique de la collectivité.

MEGALIS proposera une réunion de présentation des différents documents et une session de travail pour relecture ou accompagnement à la complétion des documents.

Durant la phase du parcours d’accompagnement des clefs USB de sensibilisation seront transmisses par l’intermédiaire de MEGALIS à la COLLECTIVITE afin de sensibiliser les personnels de celle-ci au type de menace que constitue l’usage de matériel non conforme. Les clés seront récupérées par MEGALIS à la fin du parcours.

Il est entendu que la COLLECTIVITE apportera une vigilance particulière au matériel fourni dans le cadre de cette action et notamment quant à la perte ou vol dudit matériel.

Au titre du parcours 2, une prestation en lien avec une opération de scan de vulnérabilité sera proposée à la COLLECTIVITE. Pour ce faire l’opérateur technique fournira à MEGALIS un boitier dénommé sonde réseau. MEGALIS aura la charge de connecter cette sonde sur le réseau informatique de la collectivité. L’objectif de ce boîtier sonde réseau est d’évaluer les vulnérabilités potentielles des mots de passe utilisés, des postes de travail et des serveurs le cas échéant.

La sonde réseau sera déconnectée par MEGALIS et restituée à l’opérateur technique à la fin la période de scan.

Le SIB procèdera à l’analyse des 10 vulnérabilités les plus critiques identifiées au cours du test.

Le parcours sera encadré par une réunion de lancement et une réunion de restitution. Cette dernière sera l’occasion de restituer les livrables afférents aux actions réalisées.

## Choix du parcours par la collectivité

🞏 Parcours 1 (toutes les collectivités) 🞏 Parcours 2 (commune < 3500 hab. ou EPCI < 20000 hab.)

# Phasage et durée de l’accompagnement

Un parcours ne pourra dépasser une durée de 3 mois.

Suite à la réunion de lancement un planning des différentes actions à réaliser sera défini d’un commun accord entre MEGALIS et LA COLLECTIVITE.

# intervenants

Les missions seront conduites par :

* Le chargé de mission Accompagnement cybersécurité de MEGALIS – cybersecurite@megalis.bretagne.bzh ,
* L’agent ou l’élu référent désigné par la COLLECTIVITE :
	+ NOM :……………………………………………
	+ PRENOM :………………………………………
	+ Fonction :……………………………………………………….
* Un ou des agents de l’opérateur technique ayant l’expérience suffisante pour assurer les prestations,

MEGALIS sera le point d’entrée unique pour la COLLECTIVITE et pour le suivi de l’ensemble des actions réalisées.

# Livrables

Mégalis délivrera les résultats du parcours 1 Cyber Sensibilisation :

* Les résultats de la campagne de phishing
* Les résultats de l’utilisation du module e-learning

Mégalis délivrera les résultats du parcours 2 Cyber Sensibilisation enrichi :

* Les résultats des utilisations des clefs USB
* Une restitution des vulnérabilités avec une préconisation d’action sur les 10 les plus critiques.

Mégalis fournira également :

* Les documents modèles utilisés lors du pré-audit :
	+ La fiche Identité collectivité,
	+ Le questionnaire dit « prestataire »,
	+ Le questionnaire dit « sécurité des services ».
* Les conclusions du pré-audit présentées lors d’une restitution avec une préconisation d’action sur les 5 manquements les plus critiques.

**Un kit documentaire** sera fourni à la collectivité requérante comprenant :

* Des supports de présentation Mégalis,
* Des liens vers des guides et catalogues accompagnement (Cybermalveillance.gouv.fr, ANSSI, ...)
* Des modèles de procédures
* Le catalogue de prestations de l’opérateur technique

# RESPONSABILITES

Il est particulièrement pertinent de préciser le rôle de chacun et l’étendue de sa mission dans les parcours à l’aide d’un outil de coordination et de communication de référence. Ce document est dénommé RACI. Il est associé en annexe du présent document.

MEGALIS s’engagent à réaliser les actions exclusivement pendant les jours ouvrés, du lundi au vendredi, pendant la plage horaire 8h-18h.

Durant toute la validité des tests, l’opérateur technique s’engage à prendre toutes les précautions nécessaires pour conduire les tests.

# CONFIDENTIALITE

MEGALIS s’engagent à ne divulguer aucune information à des tiers concernant les éléments récupérés suite aux actions réalisées

Dans le cadre des actions réalisées, aucune atteinte, modification ou copie des données ne serait être entreprise MEGALIS.

L’opérateur technique s’engage à respecter les conditions de confidentialité du présent article.

A la fin des parcours d’accompagnement, l’ensemble des données est supprimé.

# rÈglement des litiges

En cas de difficulté relative à la conclusion, l’exécution, l’interprétation, ou la cessation du présent contrat, les parties s’efforceront de trouver une solution amiable. En l’absence de conciliation, les parties retrouveront leur liberté et pourront saisir la juridiction compétente.

# DISPOSITIONS DIVERSES

Après signature de la présente convention, les parties concernées seront destinataires d’une copie de celle-ci.

|  |  |  |
| --- | --- | --- |
| Fait en deux exemplaires, | Pour MEGALISLeLe PrésidentLoïg CHESNAIS-GIRARDPour le Président et par délégationLe Vice-Président déléguéStéphane PERRIN | Pour la COLLECTIVITE,Le  |