Article 1 Objet

La région Bretagne propose des services de cybersécurité dans le cadre de la création du centre de réponse à incidents régional Breizh Cyber soutenu par l'État. Le présent contrat a pour objet de décrire les services proposés et les conditions de ces services.

Sont éligibles aux services de Breizh Cyber toutes entités dont tout ou partie de l'activité se réalise en Bretagne.

Article 2 Description des services proposés

Les prestations de services de cybersécurité de la région Bretagne sont opérées par le service Breizh Cyber. En plus du service gratuit d'assistance aux victimes de cyberattaque, Breizh Cyber propose les services payants proactifs détaillés dans le tableau ci-dessous.

Services inclus dans les packs d'abonnement TRIAD et TRIAD Plus

Service	Objectif
Analyse de vulnérabilités	Détecter les failles de sécurité sur vos systèmes d'information exposés sur Internet avant qu'elles ne soient exploitées par des attaquants et vous permettre de prendre les mesures de correction nécessaires afin de renforcer la posture de sécurité de votre organisation.
Évaluation du risque humain	Evaluez l'état réel de la menace, grâce à un diagnostic continu, et supervisez l'exposition cyber de vos dirigeants et collaborateurs, afin de prévenir les attaques par ingénierie sociale : usurpation d'identité et de compte, fuites de données, hameçonnage ciblé, arnaques, fraudes etc.
Veille en cybersécurité	Rester informé des dernières vulnérabilités découvertes dans les logiciels, les systèmes et infrastructures utilisées par votre organisation et vous permettre d'agir rapidement pour appliquer les mesures de sécurité nécessaires afin de réduire les risques d'exploitation de ces vulnérabilités par des attaquants.

Services indépendants DENN et RESK

Service	Objectif
DENN : audit détaillé de la surface d'exposition externe	Découvrir ce que votre organisation expose en ligne par une cartographie de votre exposition (sous-domaines, IPs, ports, site-web…), une identification des technologies et versions utilisées et des tests et vérifications de sécurité (vulnérabilités, mauvaises pratiques, oublis…)
RESK : détection de fichiers malveillants sur la messagerie et kiosque	Détecter des fichiers potentiellement malveillants attachés à vos messages courriels, contribuant ainsi à prévenir les incidents de sécurité et à réduire les risques associés aux logiciels malveillants ou au travers d'un portail.

Ces services sont opérés au moyen de solutions logicielles développés par des éditeurs de cybersécurité français.

Article 3 Abonnement aux services des packs TRIAD et TRIAD Plus

Le modèle de service est celui de la forme d'un abonnement annuel selon une formule unique pour les 3 services du pack. L'abonnement est forfaitaire.

L'abonnement débutera à la conclusion de ce contrat pour une durée de 1 an et sera reconduit par tacite reconduction à la date anniversaire du contrat. L'exécution des services est soumise à la signature préalable du présent contrat et à l'acquittement de l'abonnement.

Article 4 Services DENN et RESK

Le service DENN est le service d'audit détaillé de la surface externe. L'achat est forfaitaire à l'unité.

Le service RESK est le service de détection de fichiers malveillants de la messagerie. Il s'agit d'une licence annuelle. Il nécessite des prérequis techniques notamment que le service de messagerie électronique soit compatible avec la solution technique de l'éditeur. Ces prérequis sont vérifiés au préalable de toute commande.

Article 5 Conditions d'exécution des services pour les packs TRIAD et TRIAD Plus

La délivrance des services nécessite une réunion initiale permettant la collecte des informations nécessaires à l'exécution des prestations. Par ailleurs, des réunions de suivi sont proposées de la manière indicative suivante selon la taille de l'organisation. Les réunions sont organisées en distanciel.

Réunions de suivi / nombre de salariés	**1 à 49**	**50 à 99**	**100 à 249**	**250 à 499**	**> 500**
Fréquence des réunions de suivi	Semestrielle	Semestrielle	Semestrielle	Semestrielle	Semestrielle

Article 6 Périodicité des services proposés pour les packs TRIAD et TRIAD Plus

Chaque prestation sera executée selon la fréquence indicative suivante en fonction de la taille de l'organisation.

Service / nombre de salariés	**1 à 49**	**50 à 99**	**100 à 249**	**250 à 499**	**> 500**
Analyse de vulnérabilités (*)	Trimestrielle	Bimestrielle	Mensuelle	Mensuelle	Mensuelle
Évaluation du risque humain	Semestrielle	Semestrielle	Semestrielle	Quadrimestrielle	Quadrimestrielle
Veille en cybersécurité	Hebdomadaire	Hebdomadaire	Hebdomadaire	Hebdomadaire	Hebdomadaire

(*) En cas de parution d'une nouvelle vulnérabilité activement exploitée par des groupes d'attaquants, une campagne de recherche exceptionnelle sera effectuée.

Article 7 Coût de l’abonnement aux services

Le prix de la prestation dépend de la grille tarifaire en vigueur au moment de la souscription de l’abonnement (cf annexe 1). Le tarif acquitté au moment de la souscription ne sera pas révisé en cours d’année. En cas d’évolution de la grille tarifaire, la reconduction sera soumise à l’acceptation expresse du nouveau tarif applicable. Pour les services indépendants, le prix est indiqué et forfaitaire.

Article 8 Conditions de facturation et de paiement

Le client paiera 100 % du prix dans les 30 jours suivant la signature du présent contrat. Une facture sera émise par courrier éléctronique. Sauf mention spécifique, le règlement s’effectue de manière dématérialisée.

Article 9 Défaut de paiement

L’utilisation du service étant subordonnée à l’acquittement de l’abonnement, tout défaut de paiement entraînera la suspension du service si la relance du client est demeurée sans effet.

Article 10 Résiliation

Le présent contrat pourra être résilié à tout instant par chacune des parties, sous la réserve d'un préavis de trente jours. Dans cette hypothèse, les sommes déjà perçues par Breizh Cyber lui demeureraient acquises et le client pourrait faire l'usage le plus libre des informations qui lui auraient été communiquées, ou des documents d'ores et déjà remis.

En cas de manquement d’une partie à une quelconque de ses obligations, la résiliation prendra effet au terme d’un délai de trente jours après mise en demeure de la partie défaillante d’exécuter ses obligations, par lettre recommandée avec avis de réception.

Article 11 Modifications

Toute modification des termes du présent contrat doit faire l’objet d’un avenant écrit entre les parties, conclu dans les même formes et conditions que le présent contrat.

Article 12 Limitation de responsabilités

12.1 – Quant à l’utilisation du service

Le client s’engage, sous peine de résiliation du présent contrat, à n’utiliser les services que pour ses propres besoins.

12.2 – Quant aux incidents techniques, pannes, cyberattaques

Breizh Cyber veille à mettre en œuvre tous les moyens à sa disposition pour assurer sa mission de conseil auprès du client.

Breizh Cyber ne pourra toutefois pas être tenue pour responsable des défaillances du système d’information du client, y compris du fait d’incidents dûs à l’exécution des recommandations formulées lors d’une prestation, ni du succès d’éventuelles attaques subies par le client que Breizh Cyber n’a pour vocation que de contribuer à prévenir, ni de tout autre cas présentant un caractère de force majeure.

Article 13 Obligation de confidentialité

Chacune des parties s'engage à ne pas divulguer, ni communiquer, ni laisser divulguer ou laisser communiquer, ni utiliser directement ou indirectement, à moins qu'il n'y ait été autorisé préalablement et par écrit par l'autre partie, les renseignements, données, documents, méthodes et savoir-faire dont le secret est protégé par la loi. Ces informations excluent toute information dont une partie était déjà en possession à la date de communication de l'information par l'autre partie ainsi que toute information qui tomberait après sa communication dans le domaine public, sans que cela ne soit imputable à l'une ou l'autre des parties.

Conformément à sa RFC 2350, Breizh Cyber conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.

Article 14 Protection des données à caractère personnel

La Région Bretagne est responsable des traitements portés par Breizh Cyber : Conseil Régional de Bretagne, Collectivité territoriale de Région, immatriculée sous le numéro 233 500 016, ayant son siège au 283 Avenue Général Patton, CS 21101 35700 RENNES représentée par sa présidence.

Le responsable de traitement a nommé un Délégué à la Protection des Données (DPD). Ce dernier a pour mission de veiller au respect des dispositions de la règlementation sur la protection des données à caractère personnel. Le DPD est consulté préalablement à la création, la mise en œuvre ou la modification d'un dispositif impliquant le traitement de données à caractère personnel. Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de la Région Bretagne au fur et à mesure de leur mise en œuvre.

Le DPD veille au respect des droits des personnes (droit d'accès, de rectification, d'opposition, d'effacement, de limitation du traitement et de portabilité le cas échéant). Afin d'exercer ces droits, les personnes concernées peuvent saisir le DPD par email à l'adresse suivante informatique-libertes@bretagne.bzh.

Les droits et obligations des parties relatifs à la protection des données personnelles figurent en annexe RGPD.

Article 15 Destination des données à caractère personnel

En interne, les destinataires des données sont les personnes habilitées à les traiter dans les services de la Région Bretagne. Le responsable de traitements ne loue pas, ne cède pas et ne vend pas les données à caractère personnel des usagers, y compris à des fins de prospection commerciale. En revanche, les données à caractère personnel peuvent faire l'objet d'un traitement au nom et pour le compte de la Région Bretagne par des prestataires de services de confiance. La Région Bretagne peut notamment transférer des données personnelles au partenaire en charge des vérifications de compromission des identifiants.Dans cette hypothèse, la Région Bretagne s'assure que tous les prestataires avec lesquels elle travaille préservent la confidentialité et la sécurité des données.

Article 16 Litiges

En cas de litige relatif à l'interprétation ou à l'exécution des prestations, les parties s'efforceront de rechercher un accord amiable. En cas de désaccord persistant, le litige sera soumis à l'appréciation de la juridiction compétente.

L'adhérent

La région Bretagne,
représentée par M. Loig CHESNAIS-GIRARD
en sa qualité de Président du Conseil régional