MARCHE DES ASSURANCES
CONTRATS D'ASSURANCES POUR LE GROUPE 3iL

Marché en procédure adaptée soumis aux dispositions des articles L.2123-1 et R.2123-4 et R.2123-5 du code de la commande publique

CCTP LOT N°4 : CYBER RISQUES

Date limite de réception des dossiers : **MARDI 1 DECEMBRE 2026**

Heure limite de réception des offres : **12 h 00**

Lieu de réception des offres :

Profil acheteur : https://www.marches-publics.gouv.fr

SOMMAIRE

I. Données administratives……3

II. Evènements à garantir……4

III. Capitaux à garantir……5

IV. Antécédents……5

CLAUSE DE PREFERENCE

Les clauses d'exclusions énoncées aux documents explicatifs de la rédaction de l'assureur (conditions générales, conditions spéciales, conditions particulières etc.…) s'appliqueront de plein droit ***mais toujours dans la plus stricte limite de leur non-contradiction avec ce qui est énoncé aux CCAP et/ou CCTP sauf mentions spéciales précisées dans la liste exhaustive des réserves référencées en annexe à l'acte d'engagement.***

Le présent cahier des charges s'interprétera donc toujours en faveur des assurés quelles que soient les clauses et/ou conditions contraires et/ou limites moins favorables aux assurés qui pourraient figurer aux autres documents explicatifs de la rédaction ***sauf la stricte application des éventuelles réserves et/ou limites de l'assureur précisées exhaustivement en annexe à l'acte d'engagement*.**

I – DONNEES ADMINISTRATIVES

SOUSCRIPTEUR	**GROUPE 3iL**
DATE D'EFFET	**1ER JANVIER 2027**
DUREE DU CONTRAT	**5 ANS AVEC FACULTE DE RESILIATION**
ECHEANCE ANNUELLE	**1ER JANVIER**

DESCRIPTIF DES RISQUES

QUESTIONNAIRE SIMPLIFIE

En tant qu'établissement d'enseignement supérieur spécialisé dans les technologies de l'information, nous appliquons une politique de sécurité stricte qui nous interdit de divulguer publiquement les informations techniques et stratégiques relatives à l'architecture de notre système d'information.
La prévention, l'évaluation et la gestion globale de notre risque cyber sont intégralement pilotées par notre Direction des Systèmes d'Information (DSI) interne.
Les réponses apportées ci-dessous ont donc pour objectif de vous garantir la robustesse et la conformité de nos dispositifs de protection, tout en préservant la confidentialité vitale de nos infrastructures.

1) Mode de protection du système d'information y compris la messagerie électronique

Notre système d'information bénéficie d'une solution de sécurité complète et multicouche qui répond à l'ensemble de nos exigences de protection. Ce dispositif global sécurise nos infrastructures réseaux, nos accès, ainsi que notre environnement de messagerie électronique via un filtrage avancé contre les menaces.

2) Type d'équipement pare-feu et outil anti-spam,

Nous sommes équipés de pare-feu matériel de nouvelle génération (NGFW) fournis par l'un des leaders du marché, assurant l'inspection profonde des paquets. Le flux de messagerie est quant à lui filtré par une solution de sécurité de classe entreprise (anti-spam, anti-phishing, anti-malware) intégrée à notre environnement.

3) Politique en place pour la gestion des mots de passe, (majuscule/minuscule/chiffre/signe) avec changement périodique

Une politique de mots de passe stricte est appliquée de manière centralisée. Elle impose une forte complexité couplée à une stratégie de rotation périodique. De plus, pour garantir un niveau de sécurité optimal et contrer les compromissions d'identifiants, l'accès à nos systèmes d'information est renforcé par le déploiement de l'authentification multifacteur (MFA).

4) Logiciel antivirus utilisé

Nous appliquons une stratégie de protection des terminaux (Endpoint) adaptée au niveau d'exposition au risque, qui s'articule autour de deux scénarios de déploiement :

Pour les postes internes : L'ensemble du parc sédentaire et de nos serveurs est protégé par une solution centralisée de bout en bout de niveau professionnel (Antivirus/EDR), avec des mises à jour et une supervision continues.

Pour les postes à risques (mobilité, recherche ou télétravail) : Ces équipements bénéficient du même socle de protection, renforcé par le déploiement d'une solution de sécurité supplémentaire spécifique. Celle-ci permet de sécuriser les accès distants, de protéger les données en itinérance et de contrer les menaces dans des environnements réseaux non maîtrisés.

5) Confirmation de la réalisation des sauvegardes hebdomadaires à minima et des tests de ces sauvegardes

Nos exigences vont bien au-delà du minimum requis. Notre politique de continuité d'activité s'appuie sur une stratégie de résilience stricte basée sur une méthodologie 3-2-1-1. Les données critiques bénéficient de mécanismes de sauvegarde et de réplication en temps réel, adossés à des clusters de serveurs hautement disponibles. Pour parer à tout risque de sinistre majeur, les données sont externalisées sur un second site distant et géographiquement déporté. Afin d'éviter tout point de défaillance unique (SPOF), cette architecture repose sur le déploiement de technologies multiples et hétérogènes. Enfin, l'intégrité des données et l'efficacité des processus de reprise sont garanties par la réalisation régulière de tests de restauration.

6) Sous-traitance de tout ou partie de l'exploitation de son système d'information

L'exploitation, la sécurité et la gouvernance du cœur de notre système d'information (infrastructures, réseaux, données critiques) sont intégralement assurées et pilotées en interne par notre DSI. Le recours à la sous-traitance ou à l'externalisation est strictement limité à des services spécifiques et bien délimités, à savoir notre système de téléphonie ainsi que certaines applications de gestion métier (Ressources Humaines, gestion des engagements, etc.). L'ensemble de ces prestataires externes est encadré par des contrats de services incluant des clauses de sécurité et de confidentialité rigoureuses.

7) Collecte ou traitement des données de type bancaire, médicale, relatives à la propriété intellectuels et/ou personnelles

Dans le cadre strict de nos activités d'établissement d'enseignement supérieur, nous collectons et traitons des données personnelles (concernant les étudiants, les collaborateurs et les partenaires). L'ensemble de ces traitements est cartographié et hautement sécurisé. Un référent RGPD est identifié dans la structure.

8) Traitement de moins de 10 000 données par an

Le volume de nos flux (dossiers étudiants, gestion des diplômés, relations entreprises, environnements pédagogiques) dépasse ce seuil.

9) Présence un responsable SSI

Oui. Le DSI a la charge de la sécurité des systèmes d'information.

10) Désignation d'un délégué à la protection des données

Nous avons une personne spécifiquement désignée pour la gestion et la protection des données qui veille à notre conformité réglementaire (référent RGPD).

II – EVENEMENTS A GARANTIR

Les garanties du présent contrat ont pour vocation d'intervenir dans les cas suivants :

Acte de malveillance informatique envers votre système d'information (système informatique et/ou de données) perturbant le bon fonctionnement de celui-ci, son objet, ou le maintien de son intégrité

Et :
D'organiser et prendre en charge les mesures nécessaires pour faire face à une situation de crise.
D'indemniser :

- Les dommages, frais et pertes subis par la collectivité à la suite d'une atteinte au système d'Information y compris les extorsions de fonds et les frais supplémentaires d'exploitation
- Les dommages, frais et pertes encourus par la collectivité à la suite d'une réclamation d'un tiers.

III – CAPITAUX A GARANTIR

OFFRE DE BASE :

OBJET DE LA GARANTIE	MONTANT DE GARANTIE	FRANCHISE
GESTION DE CRISE/ACTIONS D'URGENCE	50 000 €	NEANT
DOMMAGES, FRAIS ET PERTES SUBIS PAR L'ASSURE	1 000 000 €	NEANT
CYBER EXTORSION	500 000 €	NEANT
PERTES D'EXPLOITATION/FRAIS SUPPLEMENTAIRE D'EXPLOITATION	500 000 €	NEANT
RESPONSABILITE CIVILE A L'EGARD DES TIERS	500 000 €	NEANT

VARIANTE OBLIGATOIRE 1 :

OBJET DE LA GARANTIE	MONTANT DE GARANTIE	FRANCHISE
GESTION DE CRISE/ACTIONS D'URGENCE	30 000€	NEANT
DOMMAGES, FRAIS ET PERTES SUBIS PAR L'ASSURE	500 000€	NEANT
CYBER EXTORSION	300 000€	NEANT
PERTES D'EXPLOITATION/FRAIS SUPPLEMENTAIRE D'EXPLOITATION	300 000€	NEANT
RESPONSABILITE CIVILE A L'EGARD DES TIERS	300 000€	NEANT

IV - ANTECEDENTS

Pas d'antécédent.

FAIT A …… LE ……. / …….. / 2026

SIGNATURE ET CACHET DU CANDIDAT
Précédé de la mention lue et approuvé