

|  |
| --- |
| **DOSSIER DE CANDIDATURE****« mise en œuvre du module transformant cybersécurité »** |

|  |
| --- |
| Merci de remplir et de signer ce dossier et de le retourner **uniquement**à l’adresse transformation@grandest.fr (datée, signée et scannée) |

|  |
| --- |
| COORDONNEES DE LA STRUCTURE |
| Raison sociale (inscription KBIS) |  |
| Adresse |  |
| CP et Ville |  |
| N° Siret |  |
| Code APE |  |
| COORDONNEES DE LA PERSONNE CONTACT |
| Nom – Prénom |  |
| Fonction |  |
| Tél |  |
| Mail |  |
| PRESENTATION DE LA STRUCTURE |
| Historique :Effectif (ETP) :*Précisez le nombre de salariés ayant des compétences en cybersécurité qui seront mobilisés pour le module cybersécurité.* Chiffre d’affaires n-1 :% du chiffre d’affaires réalisé avec des entreprises industrielles/BTP/logistique :*Joindre obligatoirement les bilans et comptes de résultats des 2 derniers exercices clos.*Appartenance à un groupe ?[ ]  oui [ ]  nonSi oui, lequel : Domaines d’activités :Principaux clients et leurs secteurs d’activités :Moyens techniques et humains :*Il est notamment demandé aux entreprises/opérateurs soumissionnaires de présenter l’adéquation de leurs ressources et moyens avec les attentes du module Cybersécurité (préciser le cas échéant les moyens techniques établis dans le Grand Est).**Il est demandé de joindre obligatoirement les profils des intervenants proposés pour la mise en œuvre des modules (préciser le cas échéant les profils établis dans le Grand Est, les profils internes, les éventuels profils de partenaires externes) : CV + certifications ou labels individuels en cybersécurité.*Certifications et labels collectifs de l’entreprise en cybersécurité : |
| POSITIONEMENT SUR LE MODULE CYBERSECURITE |
| Domaines d’expertises détaillés en cybersécurité (indiquez les secteurs d’activité, les tailles d’entreprises ou domaines de cybersécurité plus spécifiquement maitrisés par vos ressources) :Expériences/accompagnements déjà réalisés en cybersécurité :*Pour ce dernier point, les candidats doivent justifier :**- du nombre de projets accompagnés ou développés sur les 18 derniers mois pour chacune des briques ;**- de la nature des services proposés ;**- du secteur d’activité des industriels accompagnés et de l’expertise technique développée [préciser un ou plusieurs aspects techniques] ;**- de la satisfaction du client qui a bénéficié de l’accompagnement ou des livrables du projet.*Implication dans des réseaux ou écosystèmes liés à la cybersécurité (préciser lesquels et votre niveau d’engagement) :Compétences et expériences d’accompagnement des entreprises selon la norme 27001 (notamment dans le cadre de la certification NIS 2) : réalisations et méthodologie : |
| POSITIONEMENT SUR LES ETAPES DES MODULES |
| (Plusieurs réponses possibles)[ ]  Phase de montée en compétences et Diagnostic Technique Avancé[ ]  Phase d’ingénierie pour préparation à la mise en œuvre des solutions |
| NOTES METHODOLOGIQUES ET D’ANALYSE |
| Description détaillée (max 2 pages par note) des méthodologies d’accompagnement proposées pour les différentes étapes :*- Note méthodologique décrivant l’organisation opérationnelle envisagée pour accompagner les entreprises dans la* phase de montée en compétences et Diagnostic Technique Avancé *(si positionnement sur cette étape du module).**- Note méthodologique décrivant l’organisation opérationnelle envisagée pour accompagner les entreprises dans la phase* d’ingénierie pour préparation à la mise en œuvre des solutions *(si positionnement sur cette étape du module).*Notes d’analyses obligatoires pour tous les répondants (max 2 pages par note) :*- Note d’analyse sur l’état de l’art en matière de cybersécurité dans les entreprises actuellement et les défis à venir.**- Note d’analyse sur la prise en compte de l’impact de souveraineté dans les mesures de cybersécurité préconisées à vos clients.* |

Fait à Cliquez ou appuyez ici pour entrer du texte

le Cliquez ou appuyez ici pour entrer une date

Signature du représentant légal

*(cachet de la structure)*