REGISTRE DES QUESTIONS

INFORMATIONS CONCERNANT L'ANNONCE

Collectivité :	Syndicat Départemental d'Elimination des Déchets de l'Aube (SDEDA)
Type d'annonce :	Avis d'appel à la concurrence
Type de procédure :	Procédure adaptée ouverte pour un montant inférieur à 90 000 euros HT
Référence :	PS_1_2025
Date de mise en ligne :	Le vendredi 04 avril 2025 à 12:35:28
Date de clôture :	Le mercredi 28 mai 2025 à 12:00:00
Titre :	prestations de services d’assurances à TROYES

REGISTRE DES QUESTIONS / REPONSES REPONDUES

Questions / Réponses

Questions / Réponses

[07/04/2025 à 15:57:19] LOT CYBER
Merci de répondre aux questions ci-dessous :
Fiche de Déclaration du Risque
Société / Collectivité :
SIRET :
Contact Société / Collectivité :
Nombre d'employés :
Chiffre d’affaires / Budget de fonctionnement :
Code NAF :
Nom de domaine :
Nom du représentant dûment autorisé par la société :

Activités :
Exercez-vous une activité dans les domaines suivants :
- Plateformes de monnaie virtuelle et de crypto-monnaie ;
- Organisations de jeux de hasard et d’argent ;
- Transports aériens ou maritimes (y compris aéroports et ports) ;
- Entreprises de production et de distribution d'eau ;
- De gaz et d'électricité ;
- Sociétés de télécommunications.

Sécurité des applications :
1) Les logiciels et OS que vous utilisez sont-ils toujours maintenus par leurs éditeurs ? (ex : pas de version Windows antérieure à Windows 10) ? Si Non, pouvez-vous lister les éventuels systèmes non maintenus avec la politique de sécurité associée.

2) Tous vos équipements sont-ils équipés d’un antivirus à jour ?
? Vos postes de travail Windows ?
? Vos serveurs Windows ?

3) Avez-vous mis en place une solution d'anti-phishing (ex : identification et blocage des emails de phishing) ? Si oui, précisez la solution utilisée.

4) Avez-vous activé un pare-feu sur tous vos systèmes exposés à l’extérieur de votre réseau ? Si oui, précisez la solution utilisée.

5) A quelle fréquence effectuez-vous les mises à jour de sécurité pour l'ensemble des logiciels que vous utilisez ? Précisions des logiciels qui ont une politique de mise à jour moins fréquente.

Sauvegarde des données et restauration :
6) A quelle fréquence effectuez-vous des sauvegardes de vos données sur des supports déconnectés et isolés de votre réseau une fois les sauvegardes effectuées ? Précisions éventuelles sur votre système de sauvegarde.

7) A quelle fréquence effectuez-vous des tests de restauration à partir de vos sauvegardes ? Précisions éventuelles sur les tests de restauration.

Sécurité des systèmes :
8) Disposez-vous d’une journalisation (logs) des évènements de sécurité (ex : accès des utilisateurs aux applications, attribution de nouveaux droits d’accès, création de nouveaux utilisateurs, etc.) pour l’ensemble

de vos ordinateurs et serveurs sur une durée d’au moins 15 jours ?

9) Avez-vous mis en place une solution centralisée de remontée et de corrélation des évènements de sécurité (logs) pour vos ordinateurs et serveurs (ex : EDR, XDR, etc.) ?

Sécurité des accès :
10) Avez-vous mis en place une authentification multi facteurs (MFA) pour l'ensemble de vos systèmes critiques internes et externes et vos accès distants ? Si Non, listez les systèmes critiques qui ne disposent pas de MFA et la politique d'accès associée.

11) Avez-vous mis en place différents niveaux de droits d'accès en fonction des besoins métier de vos utilisateurs sur l'ensemble de vos systèmes critiques ? Si Non, listez les systèmes critiques sans droits d'accès limités et la politique de sécurité associée.

12) Limitez-vous les privilèges "administrateurs" exclusivement aux utilisateurs qui en ont besoin ?

13) Confirmez-vous que vos utilisateurs ne sont pas administrateurs de leurs postes de travail ?

14) Chaque utilisateur dispose-t-il de compte nominatif pour se connecter au système d'information, aux applications métier et aux systèmes critiques de l'entreprise ?

15) Imposez-vous une connexion par VPN pour tous les accès distants à vos systèmes critiques ?

16) L'ensemble de vos mots passe sont-ils robustes (min 15 caractères incluant des capitales, minuscules, chiffres et caractères spéciaux.) ?

17) Les ports RDP (Remote Desktop Protocol) de votre réseau sont-ils fermés ?

Gouvernance :
18) Avez-vous inventorié l'ensemble de votre parc informatique (équipements, logiciels, données, accès, interconnexions avec l'extérieur, etc.) ?

19) Quel volume de données traitez-vous ?
• Volumes donnés à caractère personnel sensibles ?
? Volume données bancaires ?
? Volume données de santé ?

20) Listez les mesures de protection mises en place pour sécuriser vos données (DLP, chiffrement des données, classification des données, blocage des ports USB, etc.)

Questions / Réponses

[11/04/2025 11:11:45] Mesdames, Messieurs,

Dans le cadre du lot 6 - lot CYBER - pour des raisons de confidentialité, les éventuels candidats souhaitant poser des questions ou obtenir les réponses aux questions déjà posées par d'autres sociétés, devront en faire la demande sur la boite contact@sdeda.fr et s'identifier.

Bien cordialement
Le SDEDA