REGISTRE DES QUESTIONS

INFORMATIONS CONCERNANT L'ANNONCE

Collectivité : Communauté de Communes de la Porte des Vosges Méridionales

Type d'annonce : Avis d'appel à la concurrence

Type de procédure : Appel d'offres ouvert

Référence : ass2026

Date de mise en ligne : Le jeudi 15 mai 2025 à 16:09:38

Date de clôture : Le lundi 07 juillet 2025 à 12:00:00

Titre : marché public de prestations d'assurances

Descriptif : La communauté de communes de la Porte des Vosges Méridionales procède à une consultation pour la souscription de contrats d'assurances

REGISTRE DES QUESTIONS / REPONSES REPONDUES

Questions / Réponses
[20/06/2025 à 15:55:32] Bonjour, Grâce aux questionnaires déjà transmit nous avons pu compléter une partie du notre, toutefois quelques questions restent sans réponse, pouvez-vous nous dire si : ? Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité pour la protection des terminaux EPP ? ? Vos sauvegardes sont-elles testées régulièrement ? ? Utilisez-vous une authentification mutificateurs (MFA) pour l'ensemble des accès à distance et la messagerie ? ? Avez-vous déployé un Endpoint Detection and Response (EDR) ou un Managed Detection and Response (MDR) sur l'ensemble de vos équipements informatiques ? ? Organisez-vous des formations sur l'ingénierie sociale et des tests de phishing pour tous les employés ? ? Avez-vous déployé une solution de filtrage des e-mails pour les liens ou pièces jointes malveillants, y compris la possibilité de tester et d'évaluer automatiquement les pièces jointes dans un espace dédié ? ? Combien d'atteinte au données et/ou à la sécurité su système informatique votre collectivité a-t-elle fait l'objet au cours des 36 derniers mois ? En vous remerciant par avance. Bien cordialement.

Questions / Réponses

[24/06/2025 08:23:00] Bonjour voici nos réponses :
Actuellement la solution déployée est Sentine One EDR, licence valide et à jour.
A compter du 01/09/2025, les sauvegardes seront testées mensuellement.
Les accès distants et messagerie sont protégés par MFA.
Un EDR est déployé, il s'agit de Sentinel One.
Nous prévoyons la mise en place de formations et de tests de phishing dernier trimestre 2025.
Actuellement il n'y a pas de solution de filtrage des emails et d'évaluation automatique des pièce jointes.
Aucune atteinte de données au cours des 36 derniers mois selon les éléments que je possède à ce jour.
Bien cordialement

[19/06/2025 à 14:32:15] Bonjour,

1-Pouvez-vous nous indiquer si certains véhicules sont concernés par un usage spécifique:
Transport Public de voyageurs, Bennes à ordures Ménagères, Véhicules susceptibles d'intervenir en situation d'urgence (ambulance, pompier, police, protection civile), Véhicules donnés en location, véhicules électriques dont les batteries sont en location et valeur de ces batteries ou Véhicules circulant sur un aéroport.
Merci de nous préciser les immatriculations pour les véhicules concernés.

2- Si la collectivité est concernée par du Transport Routier de Marchandises Dangereuses ?

3-Concernant le lot Flotte, merci de nous indiquer la valeur et le PTAC de la tondeuse TUFF TORQ
Bien cordialement,

[23/06/2025 08:47:13]
Bonjour, veuillez trouver ci dessous nos réponses. Bien cordialement
1-Pouvez-vous nous indiquer si certains véhicules sont concernés par un usage spécifique: NON
Transport Public de voyageurs, Bennes à ordures Ménagères, Véhicules susceptibles d'intervenir en situation d'urgence (ambulance, pompier, police, protection civile), Véhicules donnés en location, véhicules électriques dont les batteries sont en location et valeur de ces batteries ou Véhicules circulant sur un aéroport.
Merci de nous préciser les immatriculations pour les véhicules concernés.

2- Si la collectivité est concernée par du Transport Routier de Marchandises Dangereuses ? NON

3-Concernant le lot Flotte, merci de nous indiquer la valeur et le PTAC de la tondeuse TUFF TORQ : la tondeuse date de 2012, valeur d'origine 3800 € pas de carte grise

[12/06/2025 à 16:43:14] LOT CYBER
Merci de nous indiquer le montant du budget de fonctionnement correspondant à la REGIES DES EAU ET DE L'ASSAINISSEMENT ?

[12/06/2025 17:27:37] bonjour Monsieur,
Pour l'eau potable 3 600 000 €
Pour l'assainissement 3700 000 €
Bien cordialement

Questions / Réponses

[11/06/2025 à 15:50:38] LOT CYBER
Bonjour,
Nous avons pris soin d'analyser votre questionnaire et de le croiser avec celui de la compagnie.
Nous souhaitons cependant quelques précisions concernant votre politique de sauvegarde. Afin d'être éligible à un contrat d'assurance cyber il est nécessaire de disposer d'au moins une sauvegarde hors des locaux de l'entreprise ou déconnectée du réseau.

En vous remerciant par avance,

Vous avez indiqué que votre politique de sauvegarde est en cours.
Pouvez-vous nous préciser si ces sauvegardes seront effectives d'ici la mise en place du marché assurance cyber ?

• Sur des supports de stockage conservés en dehors des locaux de l'entreprise
OUI ? NON ?

• Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud)
OUI ? NON ?

• Sur des supports déconnectés des postes informatiques
OUI ? NON ?

[17/06/2025 08:17:40]
Madame Monsieur, veuillez trouver ci après nos réponses . Bien cordialement

Pouvez-vous nous préciser si ces sauvegardes seront effectives d'ici la mise en place du marché assurance cyber ?
OUI
• Sur des supports de stockage conservés en dehors des locaux de l'entreprise
OUI ?

• Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud)
NON ?

• Sur des supports déconnectés des postes informatiques
OUI ?

[26/05/2025 à 15:00:05] Bonjour,
Merci de nous préciser le nombre d'emplacements pour le terrain de camping.

[27/05/2025 16:53:13] Madame, Monsieur,
La Communauté de communes dispose de trois aires de camping car et pas de campings. L'aire de Remiremont compte 31 emplacements, Dommartin, 6 et Saint Nabord est juste une aire de vidange. Bien cordialement

Questions / Réponses

[19/05/2025 à 16:34:55] Bonjour

Pour le lot protection juridique

La stat sinistres transmise ne correspond pas à celle de la protection juridique.
merci de communiquer la stat

cdt

Je te remercie de me transmettre celle de la PJ

[19/05/2025 16:50:03] bonjour je viens de déposer le relevé de sinistralité du lot protection juridique (assurance PILLIOT). Bien cordialement

[16/05/2025 à 16:49:19] LOT CYBER
Bonjour
Afin de nous permettre de vous communiquer une cotation, nous vous remercions de bien vouloir compléter le questionnaire cyber ci-dessous.
En vous remerciant par avance
Cordialement,

Merci de lister les entités juridiques rattachées à la structure à assurer :
.....
.....

Ces entités partagent-elles le même système d'information que la structure principale à assurer ?
OUI ? NON ?

Combien de postes informatiques possédez-vous ? ? De 0 à 20 ?De 21 à 50 ? Plus de 50

Avez-vous un site internet ou un extranet ?
OUI ? NON ?
Si OUI :
- Le contrat d'hébergement de votre site intègre-t-il une solution anti-DDoS ?
OUI ? NON ?

- Votre site est-il un point d'accès pour vos salariés et/ou vos partenaires ?
OUI ? NON ?

- Votre site intègre-t-il des services de vente de produits et/ou de services en ligne ?
OUI ? NON ?
Si OUI à cette question, répondre aux questions suivantes :
- Votre site internet est-il sécurisé via un protocole HTTPS ?
OUI ? NON ?

- Conservez-vous les données bancaires de vos clients ou fournisseurs ?
OUI ? NON ?
-Etes-vous référencé comme sous-traitant / fournisseur dans des grandes entreprises ou des administrations ?
OUI ? NON ?

- Détenez-vous des informations soumises à une obligation de confidentialité renforcée (*) (secret des affaires, secret professionnel ou secret médical) dans votre système informatique ?
OUI ? NON ?
(*) C'est-à-dire :
L'attaque d'un système informatique aura des conséquences majeures si celui-ci contient des données très sensibles protégées par le secret des affaires (au sens de la directive européenne sur le secret des affaires, votée en avril 2016). A titre d'exemple, des secrets de fabrication dans le monde industriel ou des données relatives à une affaire chez un avocat constituent des données à caractère confidentiel.

Si OUI à cette question, répondre à la question suivante :

- Ces informations concernent-elles des tiers (par exemple, vos clients, vos sous-traitants ou vos fournisseurs…) ?
OUI ? NON ?

Votre réseau interne est-il protégé des connexions externes (firewall) ?
OUI ? NON ? Ne Sait Pas ?

Avez-vous des outils de filtrage réseau sur votre système informatique ?
OUI ? NON ? Ne Sait Pas ?

Avez-vous mis en place un plan de continuité d'activité (PCA) traitant de l'indisponibilité de votre système informatique ?
OUI ? NON ? Ne Sait Pas ?

A quelle fréquence les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?

Une seule réponse possible
? Quotidiennement
? Hebdomadairement
? Moins fréquemment

Comment les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?
Plusieurs réponses possibles
• Sur des supports de stockage conservés en dehors des locaux de l'entreprise ?
OUI ? NON ?

• Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud) ?
OUI ? NON ?

• Sur des supports déconnectés des postes informatiques ?
OUI ? NON ?

Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité ?
OUI ? NON ?
Si non, utilisez-vous un antivirus gratuit avec mise à jour régulière ?
OUI ? NON ?

Imposez-vous une mise à jour trimestrielle des mots de passe de vos collaborateurs ?
OUI ? NON ?

Avez-vous mis en place des règles de sécurisation des mots de passe ?
OUI ? NON ?

Vos collaborateurs sont-ils sensibilisés aux risques numériques et à leurs conséquences ?
OUI ? NON ?
Si OUI, précisez les dispositifs déployés dans votre entreprise :
Plusieurs réponses possibles
- Des simulations d'attaques par phishing (hameçonnage) ? OUI ? NON ?

- Des formations présentiels ou e-learning ? OUI ? NON ?

- La diffusion de guide de bonnes pratiques ? OUI ? NON ?

Avez-vous mis en place une politique ou une charte de sécurité informatique formalisée, pilotée et régulièrement communiquée à l'ensemble de vos collaborateurs ?

OUI ? NON ?

Questions / Réponses

[11/06/2025 14:29:11] Madame, Monsieur, veuillez trouver ci dessous nos réponses. Bien cordialement

entités juridiques rattachées à la structure à assurer :
.....COMMUNAUTE DE COMMUNES DE LA PORTE DES VOSGES MERIDIONALES - REGIES DES EAU ET DE
L'ASSAINISSEMENT.....

Ces entités partagent-elles le même système d'information que la structure principale à assurer ?
OUI ?

Combien de postes informatiques possédez-vous ? ? Plus de 50

Avez-vous un site internet ou un extranet ?
OUI ?
Si OUI :
- Le contrat d'hébergement de votre site intègre-t-il une solution anti-DDoS ?
OUI ? Sécurisation EDR sur l'ensemble des VMS

- Votre site est-il un point d'accès pour vos salariés et/ou vos partenaires ?
OUI ?

- Votre site intègre-t-il des services de vente de produits et/ou de services en ligne ?
NON ?
Si OUI à cette question, répondre aux questions suivantes :
- Votre site internet est-il sécurisé via un protocole HTTPS ?
OUI ?

- Conservez-vous les données bancaires de vos clients ou fournisseurs ?
OUI ?
-Etes-vous référencé comme sous-traitant / fournisseur dans des grandes entreprises ou des administrations ? NON ?

- Détenez-vous des informations soumises à une obligation de confidentialité renforcée (*) (secret des affaires, secret professionnel ou secret médical) dans votre système informatique ?
OUI ?
(*) C'est-à-dire :
L'attaque d'un système informatique aura des conséquences majeures si celui-ci contient des données très sensibles protégées par le secret des affaires (au sens de la directive européenne sur le secret des affaires, votée en avril 2016). A titre d'exemple, des secrets de fabrication dans le monde industriel ou des données relatives à une affaire chez un avocat constituent des données à caractère confidentiel.

Si OUI à cette question, répondre à la question suivante :

- Ces informations concernent-elles des tiers (par exemple, vos clients, vos sous-traitants ou vos fournisseurs…) ?
OUI ?

Votre réseau interne est-il protégé des connexions externes (firewall) ?
OUI ? firewall coeur de réseau

Avez-vous des outils de filtrage réseau sur votre système informatique ?
OUI ? via firewall

Avez-vous mis en place un plan de continuité d'activité (PCA) traitant de l'indisponibilité de votre système informatique ?
en cours

A quelle fréquence les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?

Une seule réponse possible
? Quotidiennement

Comment les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?
Plusieurs réponses possibles
• Sur des supports de stockage conservés en dehors des locaux de l'entreprise ?
NON ? mais en cours

• Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud) ?
NON ? mais en cours

• Sur des supports déconnectés des postes informatiques ?
NON ? mais en cours

Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité ?
OUI ?
Si non, utilisez-vous un antivirus gratuit avec mise à jour régulière ?
NON ?

Imposez-vous une mise à jour trimestrielle des mots de passe de vos collaborateurs ?
NON ?

Avez-vous mis en place des règles de sécurisation des mots de passe ?
OUI ?

Vos collaborateurs sont-ils sensibilisés aux risques numériques et à leurs conséquences ?
OUI ?
Si OUI, précisez les dispositifs déployés dans votre entreprise :
Plusieurs réponses possibles
- Des simulations d'attaques par phishing (hameçonnage) ? NON ?

- Des formations présentiels ou e-learning ? OUI ?

- La diffusion de guide de bonnes pratiques ? OUI ? NON ? en cours

Avez-vous mis en place une politique ou une charte de sécurité informatique formalisée, pilotée et régulièrement communiquée à l'ensemble de vos collaborateurs ?
NON ?

Questions / Réponses

[16/05/2025 à 13:32:18] 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

[11/06/2025 14:39:56] Madame , Monsieur, ci dessous nos réponses. Bien cordialement

Fiche de Déclaration du Risque
Société / Collectivité : voir dossier
SIRET : idem
Contact Société / Collectivité : idem
Nombre d'employés : 130
Chiffre d'affaires / Budget de fonctionnement : idem
Code NAF : idem
Nom de domaine : idem
Nom du représentant dûment autorisé par la société : idem

Activités :
Exercez-vous une activité dans les domaines suivants :

- Entreprises de production et de distribution d'eau ;

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. OUI

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

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. NON

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

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. FREQUENCE EDITEUR

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. QUOTIDIEN

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

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 ? en cours

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.) ? en cours

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. OUI

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. OUI

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

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

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 ? OUI

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

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

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

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

19) Quel volume de données traitez-vous ?
• Volumes donnés à caractère personnel sensibles ?
? Volume données bancaires ? logiciel de comptabilité
? Volume données de santé ? crèche 200 enfants

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.) en cours

Questions / Réponses

[16/05/2025 à 07:59:21] LOT CYBER : Bonjour, merci de nous apporter les précisions suivantes:
1/ Un logiciel antivirus est-il installé sur tous les postes de travail et serveurs Windows et est mis à jour au plus tard 15 jours après qu'une mise à jour soit disponible ?
2/ Est-ce que des sauvegardes des données et des éléments critiques de votre système informatique sont réalisées a minima toutes les semaines avec une rétention minimale de 2 semaines ; et sont des sauvegardes déconnectées, des sauvegardes immuables, ou des sauvegardes sécurisées ?
3/ Est-ce que vous collectez, traitez et stockez :
moins de 250 000 données à caractère personnel au sens du RGPD ; et
moins de 250 000 données bancaires (numéro de carte bancaire ou RIB) ; et
moins de 250 000 données à caractère sensible au sens du RGPD (notamment les données médicales) ?

Enfin et sauf erreur de notre part, les AE n'ont pas été versés au DCE. Vous remerciant d'avance pour leurs transmissions.

Bien à vous.

[19/05/2025 15:27:32] bonjour ,
oui un logiciel antivirus est installé sur tous les postes de travail et serveurs est mis à jour comme indiqué
oui sauvegardes des données et éléments critiques toutes les semaines avec rétention minimales de 2 semaines - sauvegardes copie à froid déconnectées, immuables sécurisées chiffrées et protégées.
collecte traitement et stockage de moins de 250 000 données à caractère personnel au sens du RGPD
Bien cordialement