DOCUMENT 04

Répondre à un questionnaire sécurité fournisseur

Banque de réponses modèles, dossier de preuves et méthode pour répondre vite, juste et sans sur-déclarer.

Entreprise		Date		Version	

Pourquoi vos clients vous posent ces questions

Les grands comptes, collectivités et entreprises soumises à NIS2 doivent maîtriser le risque de leur chaîne d'approvisionnement. Vous êtes un maillon : ils vous envoient donc un questionnaire de sécurité (parfois 50 à 200 questions) avant de signer ou de renouveler. Bien y répondre devient un avantage commercial.

La règle d'or : ne jamais sur-déclarer
Répondez « Oui » seulement si vous pouvez le prouver. Préférez « Partiellement » avec un plan d'action daté à un « Oui » invérifiable : un questionnaire est souvent contractuel et peut être audité. Un « Non » assorti d'une échéance de mise en conformité inspire plus confiance qu'une réponse parfaite et fausse.

Méthode en 5 étapes

1. **Qualifier** le questionnaire : périmètre (services concernés), délai, contact, standard éventuel (ISO 27001, SIG, questionnaire maison).
2. **Désigner un seul rédacteur** et un valideur (direction) ; interroger le prestataire IT sur les questions techniques.
3. **Répondre** à partir de la banque ci-dessous, en adaptant chaque réponse à votre réalité, et rassembler les preuves.
4. **Relire et valider** : cohérence avec la charte, le plan de sauvegarde et le registre RGPD.
5. **Capitaliser** : archiver les réponses validées pour le prochain questionnaire (gain de temps de 70 %).

Dossier de preuves à préparer

- [ ] Charte informatique signée (document 01) et attestation de sensibilisation des équipes.
- [ ] Plan de sauvegarde et dernier compte rendu de test de restauration (document 02).
- [ ] Registre RGPD, politique de confidentialité, contrats de sous-traitance (document 03).
- [ ] Attestation d'assurance cyber / responsabilité civile professionnelle.
- [ ] Attestations de vos prestataires clés (hébergeur, éditeur) : ISO 27001, SOC 2, HDS selon le cas.
- [ ] Rapport du dernier diagnostic ou audit de sécurité, avec plan d'action.
- [ ] Procédure de gestion des incidents (document 05) et organigramme du référent sécurité.

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

Banque de réponses modèles

Adaptez chaque réponse : remplacez les éléments entre [crochets] par votre réalité, supprimez ce qui n'est pas exact. Les cellules vertes sont modifiables dans le PDF.

Gouvernance et organisation

Question type	Réponse modèle à adapter	Preuve à joindre
Disposez-vous d'une politique de sécurité de l'information ?	[Oui / Partiellement]. Une charte informatique, signée par l'ensemble du personnel, fixe les règles d'usage et de protection des données ; elle est revue chaque année.	Charte signée
Un responsable de la sécurité est-il désigné ?	Oui. [Nom, fonction] est référent cybersécurité et RGPD, appuyé par [prestataire IT]. Il rend compte à la direction [fréquence].	Organigramme
Une analyse de risques a-t-elle été réalisée ?	[Oui / En cours]. Un diagnostic de sécurité a été réalisé le [date] selon les référentiels ANSSI/NIS2/RGPD ; un plan d'action priorisé est suivi.	Rapport de diagnostic

Contrôle d'accès

Question type	Réponse modèle à adapter	Preuve à joindre
L'authentification multifacteur (MFA) est-elle déployée ?	[Oui / Partiellement]. MFA activée sur [messagerie, VPN, comptes administrateurs, outils métier]. [Périmètre restant à couvrir : …, échéance : …].	Capture de configuration
Quelle est votre politique de mots de passe ?	Mots de passe d'au moins 12 caractères, uniques, stockés dans un gestionnaire de mots de passe d'entreprise ; changement immédiat en cas de compromission suspectée.	Charte, art. 1
Les accès sont-ils revus lors des départs et changements de poste ?	Oui. Procédure d'arrivée/départ : création au poste, retrait des droits le dernier jour, revue [semestrielle/annuelle] des droits.	Procédure RH/IT

Postes, réseau et correctifs

Question type	Réponse modèle à adapter	Preuve à joindre
Les postes sont-ils protégés contre les malwares ?	Oui. [Antivirus/EDR] déployé sur 100 % des postes et serveurs, supervisé par [prestataire], disques des portables chiffrés.	Console / attestation
Quelle est votre politique de mises à jour ?	Mises à jour automatiques des systèmes et applications ; correctifs critiques appliqués sous [15] jours ; inventaire du parc tenu à jour.	Rapport de patch
Le réseau est-il segmenté et protégé ?	[Oui / Partiellement]. Pare-feu [marque] à jour, Wi-Fi invité séparé du réseau interne, accès distants via VPN avec MFA.	Schéma réseau

Sauvegarde et continuité d'activité

Question type	Réponse modèle à adapter	Preuve à joindre
Vos données sont-elles sauvegardées ?	Oui. Sauvegardes [quotidiennes] selon la règle 3-2-1, chiffrées, dont une copie [hors ligne / immuable]. Rétention [30 jours] + archives mensuelles.	Plan de sauvegarde
Testez-vous la restauration ?	Oui. Tests de restauration [trimestriels], dernier test réussi le [date], consigné dans un journal.	Journal des tests
Disposez-vous d'un plan de continuité (PCA/PRA) ?	[Oui / Partiellement]. RPO [x h] et RTO [x h] définis pour les systèmes critiques ; procédure de reprise documentée et testée [fréquence].	Plan, document 02

Protection des données (RGPD)

Question type	Réponse modèle à adapter	Preuve à joindre
Tenez-vous un registre des traitements ?	Oui. Registre art. 30 tenu à jour, révisé [annuellement] et à chaque nouveau traitement.	Registre RGPD
Vos sous-traitants sont-ils encadrés contractuellement ?	Oui. Contrats de sous-traitance (art. 28) signés avec [x] prestataires ; garanties pour tout transfert hors UE.	Registre des sous-traitants
Où les données sont-elles hébergées ?	[Pays/région, hébergeur]. Aucun transfert hors UE sans garanties appropriées [ou : néant].	Contrats d'hébergement

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

Gestion des incidents

Question type	Réponse modèle à adapter	Preuve à joindre
Avez-vous une procédure de gestion des incidents ?	Oui. Procédure formalisée (réflexes, contacts, qualification, notification CNIL sous 72 h le cas échéant, information du client).	Fiche réflexe, doc. 05
Vous engagez-vous à nous notifier un incident ?	Oui. Nous notifions le client concerné sous [48] heures après la découverte d'un incident affectant ses données ou ses services, puis fournissons un point régulier.	Clause contractuelle
Avez-vous subi un incident au cours des 3 dernières années ?	[Oui / Non]. [Si oui : nature, date, impact, mesures correctives mises en œuvre.]	Retour d'expérience

Ressources humaines et sensibilisation

Question type	Réponse modèle à adapter	Preuve à joindre
Le personnel est-il sensibilisé à la cybersécurité ?	Oui. Sensibilisation à l'arrivée puis [annuelle] (phishing, mots de passe, signalement), avec [exercice de faux e-mail / quiz].	Attestation, support
Des engagements de confidentialité sont-ils signés ?	Oui, via le contrat de travail et la charte informatique ; clauses de confidentialité avec les prestataires.	Contrats

Sécurité physique

Question type	Réponse modèle à adapter	Preuve à joindre
L'accès aux locaux et aux équipements est-il contrôlé ?	Oui. Accès par [badge/clé], salle ou baie serveur fermée à clé, visiteurs accompagnés, [alarme/vidéosurveillance].	Procédure d'accès

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

Lettre d'accompagnement type

À joindre au questionnaire retourné.

Objet : Réponse au questionnaire de sécurité — **[Client]**

Madame, Monsieur,

Veuillez trouver ci-joint les réponses de **[Nom de l'entreprise]** à votre questionnaire de sécurité du [date]. Nous avons répondu en toute transparence : lorsqu'une mesure est partiellement en place, nous l'indiquons avec le plan d'action et l'échéance associés. Les pièces justificatives référencées sont jointes ou disponibles sur demande.

Notre référent sécurité, [Nom], reste à votre disposition pour tout complément ou échange. Nous nous engageons à vous informer sans délai de tout évolution significative de notre dispositif de sécurité.

Cordialement,

Synthèse de maturité (à compléter)

Domaine	Niveau	Principaux axes d'amélioration prévus (échéance)
Gouvernance		
Contrôle d'accès		
Postes et réseau		
Sauvegarde / continuité		
Protection des données		
Incidents		
Sensibilisation		

Niveau : Conforme · Partiel · Non couvert. Cette synthèse est utile en interne et lors des audits clients.

Vous recevez souvent ces questionnaires ?
Un diagnostic formalisé de votre maturité (ANSSI, NIS2, RGPD) fournit des réponses documentées et un plan d'action daté, réutilisables pour chaque client. **cyberdiagnostic.fr** vous le fournit en 10 minutes.

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.