Cyber-Sérénité

Offre d'assurance Cyber-Sérénité personnalisée
Formulaire de demande de souscription

Toutes les données renseignées restes confidentielles

Les informations recueillies dans le cadre de ce formulaire ont pour objectif d'évaluer la politique de sécurité de votre SI et de protection de vos données afin de vous proposer une Cyber-assurance adaptée à vos besoins, sur la base des déclarations qui seront faites. Aussi, le formulaire doit être dûment complété par une personne habilitée à engager la société.

«Toute déclaration intentionnellement fausse quant au risque à garantir peut entraîner par la suite une nullité du contrat cyber-assurance (Article L.113-8 du code des assurances).»

Nous nous engageons à vous répondre sous 8 jours

Nous vous conseillons d'enregistrer ce formulaire sur votre bureau, le remplissage de ce dernier prend environ 10 minutes

Commencer

1 Activité Entreprise

les champs avec * sont obligatoires

Identification de l'entreprise

Raison sociale de l'entreprise :

No Siret* :

Adresse :

Code Postal :

Ville :

Téléphone*:

Télécopie :

Site internet :

Adresse mail* :

Activité de l'entreprise

Activité principale de l'entreprise*

Autres activités *

Chiffre d'affaire en KE et effectif *

	ANNEE N		ANNEE N+1		ANNEE N+2	
	Effectif	CA	Effectif	CA	Effectif	CA
France						
Union Européenne						
USA/Canada						
Reste du Monde						
Total						

Périmètre à assurer : préciser si la société a des filiales à assurer

Nom de la filiale	Activité de la filiale	Chiffre Affaire	Ville/Pays

Commentaires particuliers

Avez vous pensé à sauvegarder votre formulaire ?

2 Renseignements relatifs aux données informatiques que vous traitez

Quelle est le *type de données informatiques* que vous stockez, traitez ou transmettez ?

○ OUI	○ NON	Informations d'ordre financier (compte bancaire, carte de crédit, …)
○ OUI	○ NON	Informations liées aux données personnelles (nom, prénom, adresse, no CNI, no passeport,…)
○ OUI	○ NON	Informations liées aux données marketing et commerciales
○ OUI	○ NON	Informations d'ordre médical (antécédents médicaux, no sécurité sociale, …)

Quel est le nombre de *données informatiques* que vous stockez sur votre réseau ?

Type de données/ volume	X <100	X< 1000	X< 10 000	X< 100 0000	X> 100 000
Données personnelles	○	○	○	○	○
Données clients	○	○	○	○	○
Données médicales	○	○	○	○	○
Données financières	○	○	○	○	○
Autres données	○	○	○	○	○

Quelle *politique d'information* avez-vous sur les données personnelles détenues ?

○ OUI	○ NON	Vous demandez le consentement des personnes pour disposer de leurs données personnelles et/ou les personnes sont informées du type de données que vous détenez
○ OUI	○ NON	Les personnes sont informées de la manière dont vous récupérez les données personnelles et de la durée de détention des données collectées
○ OUI	○ NON	Les personnes sont informées de l'utilisation et du traitement qui est fait de leurs données personnelles
○ OUI	○ NON	Les personnes peuvent accéder, rectifier ou supprimer les informations concernant leurs données personnelles

En cas de transfert de données personnelles à un tiers :

○ OUI	○ NON	Vous informez les personnes que leurs données font l'objet d'un transfert à un tiers
○ OUI	○ NON	Vous faites signer au tiers un engagement de respect de la politique de confidentialité des données personnelles
○ OUI	○ NON	Vous contrôlez le respect de la politique de confidentialité

Quelle *politique de protection* des données personnelles avez-vous mis en place ?

○ OUI	○ NON	Une politique de protection et de traitement des données est formalisée et approuvée par la direction
○ OUI	○ NON	Les aspects juridiques de la protection des données personnelles ont été validés
○ OUI	○ NON	Vous vérifiez régulièrement que vous êtes conforme aux lois et à la règlementation en vigueur concernant la protection des données personnelles
○ OUI	○ NON	Vous avez fait l'objet d'un audit par un organisme extérieur sur vos pratiques concernant les données personnelles dans les 2 dernières années
○ OUI	○ NON	Vous disposez d'un responsable de la protection des données en interne
○ OUI	○ NON	Vous avez mis en place des règles de sécurité concernant l'accès, l'exploitation et la transmission de données personnelles
○ OUI	○ NON	Le personnel autorisé est formé aux règles de sécurité concernant l'accès, l'exploitation et la transmission des données personnelles
○ OUI	○ NON	Le personnel autorisé a signé un engagement ou une clause de confidentialité

Quels sont les *moyens de protection* des données personnelles ?

○ OUI	○ NON	Les données sont stockées (cassette, disque, …)
○ OUI	○ NON	Les données stockées sur le réseau sont cryptées de façon standard ou systématique
○ OUI	○ NON	Les données en transit sont cryptées (email, transfert de fichiers, …)
○ OUI	○ NON	Les données des appareils mobiles sont cryptées (smartphones, portables)
○ OUI	○ NON	Les données des clés USB, DVD, … sont cryptées
○ OUI	○ NON	Autorisez-vous la copie ou le transfert des données personnelles
○ OUI	○ NON	Disposez-vous d'un outil contre la fuite de données (DLP : Data Leak Prevention) sur les systèmes

Quels sont les *contrôles d'accès* aux données personnelles ?

○ OUI	○ NON	Les données sont accessibles par tous les collaborateurs de l'entreprise
○ OUI	○ NON	Les accès physiques aux informations à caractère personnel sont limités
○ OUI	○ NON	Les accès aux informations à caractère personnel sont contrôlés et surveillés

Compléments informations si vous acceptez des *paiements par carte bancaire*

		% du chiffre d'affaire sur 12 mois réalisé par carte bancaire
○ OUI	○ NON	Les données bancaires sont stockées sur votre réseau informatique (même de façon ponctuelle ou provisoire)
○ OUI	○ NON	Si vous stockez des données bancaires, les serveurs SQL sont protégés contre les attaques par injection SQL
○ OUI	○ NON	Conformité avec les règles de PCI (Payment Card Industry)
○ OUI	○ NON	Rapport de conformité des règles PCI réalisé par une société extérieur certifiée

Si pas de conformité aux standards PCI, précisez les raisons et la date à laquelle ils seront effectifs :

Avez vous pensé à sauvegarder votre formulaire ?

3 Renseignements relatifs à la sécurité de votre système d'information

Quelle *organisation* de la sécurité de votre Système d'Information (SSI) ?

○ OUI	○ NON	Une politique de sécurité est formalisée et approuvée par la direction
○ OUI	○ NON	Une charte de bonne utilisation des services et ressources informatiques est communiquée à l'ensemble du personnel
○ OUI	○ NON	Une organisation, des rôles et des responsabilités sont définis pour la gestion de la Sécurité des Systèmes d'Information (SSI)
○ OUI	○ NON	Une campagne de sensibilisation des utilisateurs à la SSI est menée régulièrement
○ OUI	○ NON	Des audits réguliers de la SSI sont menés avec mise en oeuvre des recommandations
○ OUI	○ NON	Certification dans la gouvernance des SI (Iso 900, Iso 20000-1, Iso 27000, PCI DSS,…)

Si vous avez des certifications, merci de préciser lesquelles:

Quel *contrôle d'accès logique* aux systèmes?

○ OUI	○ NON	Un inventaire des systèmes critiques est formalisé
○ OUI	○ NON	Une procédure de classification de l'information selon son niveau de criticité (Confidentialité, Disponibilité, Intégrité) est formalisée
○ OUI	○ NON	Les tiers signent un engagement de confidentialité
○ OUI	○ NON	L'accès aux systèmes d'informations exige l'identification et l'authentification des utilisateurs
○ OUI	○ NON	La gestion du renouvellement et du durcissement des mots de passe est mise en place pour l'accès aux systèmes d'information et aux applications critiques
○ OUI	○ NON	Les autorisations d'accès sont basées sur les rôles des utilisateurs et une procédure est formalisée pour la gestion des autorisations
○ OUI	○ NON	Les systèmes critiques bénéficient de mesures de sécurité complémentaires telles que : cloisonnement, traçabilité, authentification renforcée …
○ OUI	○ NON	Les droits d'accès aux applications critiques sont revus régulièrement selon le principe du minimum de privilège

Quelle *protection* des systèmes et anti-virus ?

○ OUI	○ NON	Une configuration de référence (Masters) est utilisée pour la configuration des postes
○ OUI	○ NON	Une gestion centralisée du parc informatique est mise en place
○ OUI	○ NON	Les utilisateurs ne sont pas administrateurs de leurs postes
○ OUI	○ NON	Les portables sont protégés par pare-feu personnel ou les portables ne peuvent se connecter à Internet que via le réseau d'entreprise
○ OUI	○ NON	Un antivirus est installé sur tous les systèmes notamment Windows et l'anti-virus est mis à jour automatiquement
○ OUI	○ NON	Les patchs de sécurité sont déployés régulièrement
○ OUI	○ NON	Des tableaux de bord sont produits et suivis régulièrement
○ OUI	○ NON	Des règles de sécurité et les procédures de gestion des changements et de gestion des incidents sont définies pour la gestion, l'exploitation ou la configuration des systèmes

Quelle *gestion des sauvegardes ?*

○ OUI	○ NON	Un plan de sauvegarde est formalisé et mis à jour régulièrement
○ OUI	○ NON	Des sauvegardes au moins hebdomadaires sont réalisées
○ OUI	○ NON	Au moins une copie des sauvegardes est placée dans une autre location éloignée
○ OUI	○ NON	Les sauvegardes sont testées régulièrement
○ OUI	○ NON	Des tests de restauration des sauvegardes sont réalisés régulièrement

Cycle de rotation des sauvegardes	Durée de rétention (1)	Volume sauvegardé (Go)
Quotidienne	○	
Hebdomadaire	○	
Mensuelle	○	
Autre :		

(1) Durée avant réécriture du support de sauvegarde

Quelle *protection* du réseau ?

○ OUI	○ NON	Un pare-feu (firewall) est installé entre le réseau interne et internet, le contrôle des flux entrants et sortant est mis à jour régulièrement
○ OUI	○ NON	Les utilisateurs ont accès à internet à travers un dispositif réseau muni de l'antivirus web
○ OUI	○ NON	Les utilisateurs ont accès à internet à travers un dispositif réseau muni du filtrage de sites Web
○ OUI	○ NON	Une segmentation du réseau est mise en place pour séparer les zones critiques (serveurs, administration..) des zones moins critiques (telle que la zone bureautique)
○ OUI	○ NON	Des audits, tests de pénétrations ou analyse de vulnérabilité sont conduits régulièrement et un plan de remédiation est mis en oeuvre
○ OUI	○ NON	Des procédures de gestion d'incidents et de gestion des changements sont mises en place
○ OUI	○ NON	Des rapports de service et de performance du réseau sont produits régulièrement
○ OUI	○ NON	Une surveillance proactive contre les intrusions réseau est mise en oeuvre à l'aide de sonde de détection d'intrusion et/ou de système de corrélation des événements de sécurité …
○ OUI	○ NON	Les systèmes critiques sont placés dans, au moins, une salle informatique dédiée avec un contrôle d'accès restreint

Quelle *protection* des locaux informatiques ?

○ OUI	○ NON	Les systèmes critiques sont hébergés dans un Datacenter ou dans un local de même niveau de sécurité
○ OUI	○ NON	Les systèmes critiques sont redondés selon une architecture Actif/Passif ou Actif/Actif …
○ OUI	○ NON	Les systèmes critiques sont redondés sur deux locaux distincts
○ OUI	○ NON	La détection d'incendie dans les zones critiques est mise en place avec alarme opérationnelle reportée vers un poste de surveillance
○ OUI	○ NON	Le contrôle d'environnement (température, humidité) est mise en place avec alarme opérationnelle reportée vers un poste de surveillance
○ OUI	○ NON	Un système d'extinction automatique d'incendie est mis en place
○ OUI	○ NON	L'alimentation électrique est protégée par un onduleur (UPS) munis de batteries et maintenus régulièrement
○ OUI	○ NON	L'alimentation électrique est secourue par un générateur électrique maintenu et testé régulièrement
○ OUI	○ NON	Les dispositifs de secours, d'alarmes … sont testés régulièrement

Fonctions informatiques *externalisées*

○ OUI	○ NON	Gestion des postes de travail
○ OUI	○ NON	Gestion des serveurs
○ OUI	○ NON	Gestion du réseau
○ OUI	○ NON	Gestion de l'infrastructure sécurité
○ OUI	○ NON	Gestion des applications
○ OUI	○ NON	Traitement des données
○ OUI	○ NON	Hébergement de données

Quelle *politique d'externalisation* pour votre système d'information?

○ OUI	○ NON	Des exigences de qualité de service sont définies avec le prestataire (SLA : Service Level Agreement)
○ OUI	○ NON	Des pénalités sont appliquées en cas de non respect des exigences de qualité de service
○ OUI	○ NON	Des procédures de gestion des changements et de gestion des incidents sont définies avec le prestataire

Politique *d'externalisation* *(suite)*

○ OUI	○ NON	Des rapports de service et de performance sont fournis régulièrement par le prestataire
○ OUI	○ NON	Un comité de suivi et de pilotage est organisé avec le prestataire pour la gestion du service et son amélioration

Remarques particulières

Avez vous pensé à sauvegarder votre formulaire ?

4 Renseignements relatifs à la gestion d'un dysfonctionnement grave de votre SI

Activités *contrôlées* par le système d'information

○ OUI	○ NON	La gestion
○ OUI	○ NON	Les ventes
○ OUI	○ NON	La production

Autre (précisez)

Criticité du système d'information

Impacts d'une interruption sur l'activité	Immédiat	> 12 h	> 24 h	> 48 h	> 5 jours
Délai estimé pour reprendre les activités après une cyber-attaque ou perte de données	○	○	○	○	○
Délai estimé après lequel l'incapacité du personnel à accéder aux SI aurait un impact significatif sur l'entreprise	○	○	○	○	○
Délai estimé après lequel l'incapacité des clients à accéder au(x) site(s) web aurait un impact sur la réputation ou l'activité	○	○	○	○	○

Plan de *secours* du système d'information

En cas de défaillance du système d'information, évaluez le pourcentage du chiffre d'affaires qui pourrait être maintenu par l'application de solutions alternatives : mise en oeuvre du plan de secours, sous-traitance ou intérim, changement de processus ou de procédé

Activité(s)	% CA maintenu

Activité(s) suite	% CA maintenu

Plan de *continuité d'activité* (PCA)

○ OUI	○ NON	Une analyse des risques a été réalisée
○ OUI	○ NON	Un plan de reprise ou de continuité d'activité est formalisé et mis à jour régulièrement
○ OUI	○ NON	Une solution de secours contractuelle ou interne est identifiée
○ OUI	○ NON	Un plan de crise est défini
○ OUI	○ NON	Les systèmes et applications critiques sont redondées
○ OUI	○ NON	Des tests de secours des systèmes et applications critiques sont réalisés régulièrement

Avez vous pensé à sauvegarder votre formulaire ?

5 Renseignements relatifs à l'historique de vos sinistres en termes de cyber-risques

Quels sont les *antécédents* de votre entreprise et/ou de vos filiales en termes de cyber-risques sur les 5 dernières années ?

○ OUI	○ NON	Vous avez été victime d'une attaque virale ou d'une intrusion sur votre réseau
○ OUI	○ NON	Vous avez fait l'objet d'un vol ou d'une perte de données
○ OUI	○ NON	Votre réseau a fait l'objet d'une dégradation ou d'une intrusion
○ OUI	○ NON	Vous avez fait l'objet d'une violation de la sécurité informatique
○ OUI	○ NON	Vous avez été la cible d'un vol bancaire ou de biens électroniques
○ OUI	○ NON	Vous avez fait l'objet d'une tentative ou d'une demande d'extorsion

Si vous avez eu des antécédents, merci de préciser les circonstances, le(s) coût(s) et impact sur le chiffre d'affaire

Quelles sont les *réclamations, plaintes ou sinistres* dont votre entreprise et/ou une de vos filiales avez fait l'objet sur les 5 dernières années ?

○ OUI	○ NON	Avez-vous eu connaissance d'une réclamation ou d'une plainte à l'encontre de votre entreprise et/ou d'une de vos filiales pour atteinte à la vie privée, à la sécurité des données, à la confidentialité de données personnelles, au vol d'identité, au vol d'informations, aux droits d'auteur sur logiciels?
○ OUI	○ NON	Avez-vous eu connaissance d'une notification à des personnes d'une violation de leurs données personnelles (supposée ou avérée) par votre entreprise et/ou une de vos filiales?
○ OUI	○ NON	Avez-vous eu connaissance d'une enquête ou d'une procédure administrative à l'encontre de votre entreprise et/ou d'une de vos filiales pour atteinte à la vie privée ou à la confidentialité des données ?
○ OUI	○ NON	Avez-vous déjà ou une de vos filiales été assurée pour ce type de risque ?
○ OUI	○ NON	Si oui, avez-vous eu des sinistres pour lesquels l'assureur vous a indemnisé ?

Merci de vérifier que vous avez bien enregistré votre formulaire sur votre bureau avant de l'envoyer

Envoyer le formulaire et obtenir Votre devis Cyber-assurance sous 8 jours en cliquant sur ce bouton