**EXEMPLE DE FORMULAIRE DE QUESTIONNAIRE D'ÉVALUATION DES RISQUES FOURNISSEUR**

|  |  |
| --- | --- |
| NOM DU FOURNISSEUR | ADRESSE DU FOURNISSEUR |
|   |   |
| POINT DE CONTACT | COORDONNÉES |
|   |   |

INSTRUCTIONS: Veuillez remplir ce questionnaire dans son intégralité, en laissant des notes et en joignant des pièces justificatives si nécessaire.

**Nature du fournisseur de données aura accès à** *vérifier tout ce qui s'applique*

|  |  |  |
| --- | --- | --- |
| **X** | **TYPE DE DONNÉES** | **NOTES** |
|  | Pas d'échange de données |  |
|  | Données démographiques |  |
|  | Données financières |  |
|  | Données personnelles (par exemple, nom, adresse, numéro de téléphone) |  |
|  | Données personnelles non publiques (par exemple, SSN, médicales, propriétaires) |  |
|  | Autre:  |  |  |

**POLITIQUES ET PROCESSUS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oui** | **Non** | **N/A** | **QUESTION** | **NOTES** |
|  |  |  | Votre organisation documente-t-elle, publie-t-elle et applique-t-elle des stratégies de sécurité ? |  |
|  |  |  | Votre organisation documente-t-elle et applique-t-elle les politiques RH ? |  |
|  |  |  | Votre organisation documente-t-elle et applique-t-elle des stratégies pour l'utilisation autorisée des services en réseau ? |  |

**POURSUITE DES POLITIQUES ET DES PROCESSUS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oui** | **Non** | **N/A** | **QUESTION** | **NOTES** |
|  |  |  | Votre organisation documente-t-elle et applique-t-elle des stratégies pour l'utilisation autorisée de la messagerie, d'Internet et de l'intranet de l'entreprise ? |  |
|  |  |  | Votre organisation documente-t-elle et applique-t-elle des stratégies et des normes de chiffrement ? |  |
|  |  |  | Votre organisation documente-t-elle et applique-t-elle des politiques concernant le stockage, l'utilisation et l'élimination des données sensibles ? |  |
|  |  |  | Votre organisation documente-t-elle et applique-t-elle des politiques concernant le stockage, l'utilisation et l'élimination de données sensibles par des tiers ? |  |
|  |  |  | Votre organisation externalise-t-elle les fonctionnalités liées à la gestion de la sécurité ? |  |
|  |  |  | Les politiques et procédures respectent-elles et respectent-elles les lois et réglementations en matière de protection de la vie privée relatives à la sécurité, à la dissimulation et à la protection des données des clients? |  |
|  |  |  | Les pénalités associées à la non-conformité aux politiques de votre organisation sont-elles bien documentées? |  |
|  |  |  | [Insérer la question sur les politiques et les processus ici] |  |
|  |  |  | [Insérer la question sur les politiques et les processus ici] |  |
|  |  |  | [Insérer la question sur les politiques et les processus ici] |  |

**MESURES DE SÉCURITÉ PHYSIQUE ET DE CENTRE DE DONNÉES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oui** | **Non** | **N/A** | **QUESTION** | **NOTES** |
|  |  |  | Votre organisation examine-t-elle et évalue-t-elle régulièrement les risques physiques et environnementaux? |  |
|  |  |  | Les contrôles de périmètre des centres de données impliquent-ils l'utilisation de cartes d'accès ? |  |
|  |  |  | Les contrôles de périmètre du centre de données impliquent-ils l'utilisation de contrôles de clavier ? |  |
|  |  |  | Les contrôles de périmètre des centres de données impliquent-ils l'utilisation d'agents de sécurité ? |  |
|  |  |  | Les contrôles de périmètre du centre de données impliquent-ils l'utilisation de \_\_[ajouter une mesure ici]\_\_ ? |  |
|  |  |  | Avez-vous mis en place des procédures de continuité des activités si le bureau est inaccessible pour une raison quelconque? |  |
|  |  |  | Tous les équipements réseau sont-ils physiquement sécurisés ? |  |
|  |  |  | Votre organisation utilise-t-elle des fournisseurs de centres de données ? |  |
|  |  |  | Votre organisation utilise-t-elle les journaux des visiteurs ? Dans l'affirmative, sont-ils maintenus pendant plus de 30 jours? |  |
|  |  |  | Votre organisation maintient-elle une politique écrite concernant les exigences de sécurité physique pour le bureau? |  |
|  |  |  | [Insérez la question de sécurité physique et du centre de données ici] |  |
|  |  |  | [Insérez la question de sécurité physique et du centre de données ici] |  |

**MESURES DE SÉCURITÉ CONTRE LES LOGICIELS MALVEILLANTS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oui** | **Non** | **N/A** | **QUESTION** | **NOTES** |
|  |  |  | Tous les e-mails sont-ils analysés à la recherche de virus ? |  |
|  |  |  | Un logiciel antivirus est-il requis et activé sur tous les ordinateurs du réseau ? |  |
|  |  |  | Les logiciels antivirus ont-ils une fréquence d'analyse établie sur les ordinateurs du réseau ? |  |
|  |  |  | Votre organisation autorise-t-elle l'installation de logiciels non approuvés sur les ordinateurs du réseau ? |  |
|  |  |  | [Insérez la question de sécurité des logiciels malveillants ici] |  |
|  |  |  | [Insérez la question de sécurité des logiciels malveillants ici] |  |
|  |  |  | [Insérez la question de sécurité des logiciels malveillants ici] |  |

**MESURES DE SÉCURITÉ DE L'INFORMATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oui** | **Non** | **N/A** | **QUESTION** | **NOTES** |
|  |  |  | Votre organisation a-t-elle mis en place un programme de sécurité de l'information? (Dans la colonne des notes, veuillez fournir un lien vers toutes les politiques de sécurité et de confidentialité pertinentes destinées au public.) |  |
|  |  |  | Si votre organisation dispose d'un programme de sécurité de l'information, s'applique-t-il à toutes les opérations et à tous les systèmes qui traitent des données sensibles ? |  |
|  |  |  | Le personnel et les gestionnaires concernés sont-ils professionnellement certifiés en matière de sécurité de l'information? |  |
|  |  |  | L'accès au niveau administrateur est-il limité sur l'infrastructure réseau ? |  |
|  |  |  | Des contrôles stricts sont-ils en place pour accéder aux journaux de sécurité ? |  |
|  |  |  | [Insérer la question sur la sécurité de l'information ici] |  |
|  |  |  | [Insérer la question sur la sécurité de l'information ici] |  |
|  |  |  | [Insérer la question sur la sécurité de l'information ici] |  |

**MESURES DE SÉCURITÉ DE L'INFRASTRUCTURE RÉSEAU**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oui** | **Non** | **N/A** | **QUESTION** | **NOTES** |
|  |  |  | Votre organisation maintient-elle une stratégie de sécurité réseau ? |  |
|  |  |  | Tous les routeurs sont-ils systématisés avec des listes de contrôle d'accès pour étouffer le trafic non autorisé ? |  |
|  |  |  | Les systèmes d'exploitation serveur sont-ils corrigés au dernier niveau ? |  |
|  |  |  | Votre organisation a-t-elle mis en place un processus pour suivre et communiquer les correctifs de vulnérabilité ? |  |
|  |  |  | Votre organisation sauvegarde-t-elle vos données ? |  |
|  |  |  | Les sauvegardes sont-elles stockées et testées ? |  |
|  |  |  | Les appareils des employés sont-ils chiffrés ? |  |
|  |  |  | Un tiers est-il utilisé pour tester la sécurité de l'infrastructure réseau ? |  |
|  |  |  | Utilisez-vous des systèmes de détection d'intrusion ? |  |
|  |  |  | [Insérer la question de sécurité de l'infrastructure réseau ici] |  |
|  |  |  | [Insérer la question de sécurité de l'infrastructure réseau ici] |  |
|  |  |  | [Insérer la question de sécurité de l'infrastructure réseau ici] |  |

|  |
| --- |
| **INFORMATIONS COMPLÉMENTAIRES** |
|  |

|  |  |  |
| --- | --- | --- |
| NOM ET TITRE DE L'ÉVALUATEUR DES RISQUES | SIGNATURE | DATE |
|  |  |  |

|  |
| --- |
| **DÉMENTI**Tous les articles, modèles ou informations fournis par Smartsheet sur le site Web sont fournis à titre de référence uniquement. Bien que nous nous efforcions de maintenir les informations à jour et correctes, nous ne faisons aucune déclaration ou garantie d'aucune sorte, expresse ou implicite, quant à l'exhaustivité, l'exactitude, la fiabilité, la pertinence ou la disponibilité en ce qui concerne le site Web ou les informations, articles, modèles ou graphiques connexes contenus sur le site Web. Toute confiance que vous accordez à ces informations est donc strictement à vos propres risques. |