Relevé des prestations

Catalogue de questions aux prestataires

# À remplir par le domaine TIC/TO interne

|  |  |
| --- | --- |
| No du prestataire |  |
| Interlocuteur principal |  |
| Succursale |  |
| Activité dans les succursales |  |
| Questionnaire no |  |

# À remplir par le prestataire

|  |  |
| --- | --- |
| Nom du prestataire |  |
| Prestation fournie |  |
| Désignation professionnelle |  |
| Date |  |
| Signature |  |

# Organisation dans le secteur de la sécurité TIC

| 1.1 | Votre entreprise bénéficie-t-elle d’un certificat valable et reconnu dans le secteur informatique, tel que ISO 27001, COBIT ou une autorité officielle étrangère compétente en matière de sécurité TIC ? | oui ☐  non ☐  je ne sais pas ☐ |
| --- | --- | --- |
|  | Si oui, décrivez le certificat. |  |
| 1.2 | Comment la sécurité TIC est-elle réglée dans votre entreprise ? Décrivez les fonctions du personnel préposé à la sécurité TIC et indiquez les personnes responsables pour ce secteur (CISO, chef sécurité TIC, chef technique, etc.). |  |
| 1.3 | Connaissez-vous des lacunes de gestion ? | oui ☐  non ☐  je ne sais pas ☐ |
| 1.4 | Lorsqu’une lacune est découverte, comment se passe l’information ? Par quel canal, avec quel temps de réaction ? |  |
| 1.5 | Lorsqu’un incident TIC interne se produit, comment se passe l’information que votre entreprise donne à notre organisation ? Par quel canal, avec quel temps de réaction ? |  |

# Organisation dans le secteur de la sécurité des données

| 2.1 | Pour le traitement des données, votre entreprise respecte-t-elle les exigences et prescriptions de la loi sur la protection des données ? | oui ☐  non ☐  je ne sais pas ☐ |
| --- | --- | --- |
|  | Si non, veuillez expliquer pourquoi. |  |
| 2.2 | Votre entreprise dispose-t-elle d’un diagramme mis à jour montrant comment les données sensibles arrivent dans ses systèmes, et où elles sont finalement stockées ? | oui ☐  non ☐  je ne sais pas ☐ |
|  | Si non, votre entreprise est-elle disposée à établir un tel diagramme ? | oui ☐  non ☐  je ne sais pas ☐ |

| 2.3 | Votre entreprise utilise-t-elle des méthodes de chiffrement moderne, mises à jour, et correspondant au standard actuel, pour protéger les données sensibles lors de leur transfert entre systèmes ainsi que lors de leur stockage en ligne et dans les sauvegardes ? | oui ☐  non ☐  je ne sais pas ☐ | |
| --- | --- | --- | --- |
| 2.4 | Votre entreprise dispose-t-elle d’un concept pour la suppression définitive des données ? | oui ☐  non ☐  je ne sais pas ☐ | |
| 2.5 | Nous fournissez-vous des produits qui interviennent dans notre environnement critique ? | | oui ☐  non ☐  je ne sais pas ☐ | |
|  | Décrivez les produits TIC/TO. | |  | |

# Systèmes informatiques

| 3.1 | Votre entreprise utilise-t-elle ses propres systèmes pour nous fournir ses prestations ? | oui ☐  non ☐  je ne sais pas ☐ |
| --- | --- | --- |
|  | Si non, et si des systèmes sont mis à disposition par des tiers, de qui s’agit-il ? |  |
| 3.2 | Vos systèmes sont-ils équipés d’une solution EDR/XDR mise à jour ? Les incidents décelés par cet antivirus étendu sont-ils traités activement par votre entreprise ? Sont-ils examinés par un SOC externe ? |  |
| 3.3 | Dans quel délai pouvez-vous rétablir le fonctionnement ordinaire après une interruption des services ou une cyberattaque ? |  |

# Accès aux systèmes / appareils / ressources

| 4.1 | L’accès aux systèmes mentionnés est-il réservé uniquement à des comptes d’utilisateurs personnalisés ? | oui ☐  non ☐  je ne sais pas ☐ |
| --- | --- | --- |
| 4.2 | Votre personnel utilise-t-il, pour son travail ordinaire au quotidien, d’autres comptes d’utilisateurs que ceux autorisés pour l’accès aux systèmes mis à disposition par notre organisation ou ceux qui contiennent des données liées à notre organisation ? | oui ☐  non ☐  je ne sais pas ☐ |
| 4.3 | Votre personnel travaille-t-il selon le principe du moindre privilège ? | oui ☐  non ☐  je ne sais pas ☐ |
| 4.4 | Est-il garanti que les comptes d’utilisateurs disposant de privilèges élevés ne disposent pas en permanence de ce niveau d’autorisation ? | oui ☐  non ☐  je ne sais pas ☐ |
| 4.5 | Si des *service accounts* sont utilisés pour fournir la prestation, est-il garanti que les authentifications soient conservées en toute sécurité et ne soient pas accessibles à d’autres membres du personnel ? | oui ☐  non ☐  je ne sais pas ☐ |
| 4.6 | Les accès aux systèmes contenant ou traitant des données relatives à notre organisation sont-ils protégés par des doubles authentifications dans le cas où ces systèmes sont interrogés depuis des zones externes telles que VPN ou accès entre sites web ? | oui ☐  non ☐  je ne sais pas ☐ |
| 4.7 | Tous les accès à ces systèmes sont-ils intégrés à la journalisation et peuvent-ils être consultés sur demande par nos spécialistes TIC ? | oui ☐  non ☐  je ne sais pas ☐ |
| 4.8 | Existe-t-il une directive écrite détaillée en ce qui concerne les mots de passe ? | oui ☐  non ☐  je ne sais pas ☐ |

# Vigilance

| 5.1 | Le personnel de votre secteur de sécurité TIC a-t-il été suffisamment informé, notamment sur les questions de phishing, et leur formation a-t-elle été attestée ? | oui ☐  non ☐  je ne sais pas ☐ |
| --- | --- | --- |
| 5.2 | Le personnel de sécurité TIC de notre organisation peut-il consulter ce programme de formation ? | oui ☐  non ☐  je ne sais pas ☐ |