Auto-évaluation des risques cybersécurité

Ce questionnaire offre un premier diagnostic du niveau de cybersécurité de votre collectivité. Il est conseillé de le revoir régulièrement et de mettre en place un plan d'action pour corriger les points faibles identifiés. La cybersécurité est un processus continu qui nécessite une vigilance constante pour protéger les données des administrés et assurer la continuité des services publics.

Gouvernance de la cybersécurité

	Question	O	N
01	Avez-vous un responsable cybersécurité ou un DPO (Délégué à la Protection des Données) désigné ?		
02	Le comité de direction ou les élus sont-ils régulièrement informés des risques en cybersécurité ?		
03	Disposez-vous d'une stratégie formelle de cybersécurité pour la collectivité ?		
04	Avez-vous un plan de gestion de crise et de reprise d'activité en cas d'incident de sécurité ?		

Auto-évaluation des risques cybersécurité

Gestion des accessoires et des identités

	Question	O	N
01	Tous les utilisateurs des systèmes informatiques de la collectivité utilisent-ils des mots de passe complexes et uniques ?		
02	Les accès aux informations sensibles sont-ils restreints aux seules personnes autorisées ?		
03	Avez-vous mis en place une procédure d'authentification à double facteur (2FA) pour les accès sensibles (emails, plateformes internes) ?		

Auto-évaluation des risques cybersécurité

Sécurité des systèmes et des données

	Question	O	N
01	Tous vos systèmes informatiques et logiciels sont-ils régulièrement mis à jour pour corriger les vulnérabilités de sécurité ?		
02	Disposez-vous de pare-feu, antivirus et autres dispositifs de sécurité pour protéger vos systèmes internes ?		
03	Les données sensibles (personnelles, fiscales, etc.) sont-elles chiffrées, notamment lors de leur transmission ?		
04	Les sauvegardes de données sont-elles effectuées régulièrement et stockées de manière sécurisée ?		

Auto-évaluation des risques cybersécurité

Sensibilisation et formations des agents/élus

	Question	O	N
01	Les agents et élus reçoivent-ils des formations régulières sur les bonnes pratiques de cybersécurité ?		
02	Les agents sont-ils sensibilisés aux risques de cybersécurité, notamment concernant les emails frauduleux ou les liens suspects ?		
03	Les agents savent-ils comment réagir en cas de cyberattaque (par exemple, un phishing ou un ransomware) ?		

Auto-évaluation des risques cybersécurité

Gestion des incidents de sécurité

	Question	O	N
01	Avez-vous mis en place une procédure claire de signalement et de gestion des incidents de sécurité ?		
02	Tous les employés savent-ils comment signaler un incident de cybersécurité ?		
03	Avez-vous effectué un exercice de simulation de cyberattaque pour tester la réaction de vos agents ?		

Auto-évaluation des risques cybersécurité

Sécurisation des infrastructures et des équipements

	Question	O	N
01	Les équipements mobiles (smartphones, tablettes) sont-ils protégés par des mots de passe ou des codes PIN ?		
02	Les ordinateurs et équipements utilisés par les agents en télétravail sont-ils protégés par un VPN et des mesures de sécurité adéquates ?		
03	Avez-vous mis en place des contrôles d'accès physiques pour les équipements informatiques sensibles (serveurs, postes de travail) ?		

Auto-évaluation des risques cybersécurité

Gestion des prestataires externes

	Question	O	N
01	Les contrats avec des prestataires externes incluent-ils des clauses de cybersécurité et de protection des données ?		
02	Avez-vous vérifié la sécurité des systèmes des prestataires externes avant de leur donner accès à des informations sensibles ?		
03	Les prestataires externes ayant accès à des données sensibles respectent-ils des normes de cybersécurité adaptées ?		

Auto-évaluation des risques cybersécurité

Plan de continuité et de reprise d'activité (PCA/PRA)

	Question	O	N
01	Votre collectivité dispose-t-elle d'un Plan de Continuité des Activités (PCA) en cas d'incident de sécurité majeur ?		
02	Avez-vous un Plan de Reprise d'Activité (PRA) documenté et testé ?		
03	Les données essentielles de la collectivité sont-elles sauvegardées et peuvent-elles être restaurées rapidement en cas de perte ?		

Auto-évaluation des risques cybersécurité

Résultats

Si vous avez obtenu une majorité de **OUI** :

OUI

Vous avez une bonne base de cybersécurité en place, mais il est important de continuer à surveiller et à améliorer vos pratiques régulièrement. Nous sommes à votre disposition si vous souhaitez aller plus loin dans votre niveau de sécurité...

Si vous avez obtenu une majorité de **NON** :

NON

Il existe des lacunes dans votre stratégie de cybersécurité. Il est fortement recommandé de prendre des mesures pour renforcer la sécurité afin de réduire les risques d'incidents. Parlons-en pour voir comment améliorer votre sécurité.

Si vous avez obtenu autant de **OUI que de NON** :

OUI/NON

Vous avez mis en place plusieurs éléments de cybersécurité et c'est une excellente chose mais il vous reste encore quelques mesures d'amélioration. Parlons-en ensemble afin de vous aider à mieux protéger votre collectivité..

Auto-évaluation des risques cybersécurité

CONTACT

VOTRE DPO

SCHOETTEL Audrey
DPO externe / cybersécurité
Proche La Rochelle

www.revisium.fr

Mail : contact@revisium.fr

Tel : 0 805 035 135
ou 05 17 81 00 05