Ethias
Service commercial Collectivités
Rue des Croisiers 24, 4000 Liège
Tél. : 04 220 80 60
E-mail : secteurpublic@ethias.be

Questionnaire d'évaluation du risque

ETHIAS CYBER PROTECTION

Informations générales

Nom de l'organisation :

Adresse :

Code postal : Localité :

Secteur d'activité :

Personne de contact (personne qui signe ce questionnaire)

Raison sociale :

Nom : Prénom :

Fonction :

Tél. : Adresse mail :

2020_12_Questionnaire-CyberProtection_FR

1. Implication du Top Management

- **Avez-vous désigné un responsable du traitement et de la sécurité de l'information ?** ◯ Oui ◯ Non
- **Avez-vous identifié votre risque en matière d'ICT et protégé votre organisation pour l'avenir ?** ◯ Oui ◯ Non
- **Respectez-vous les exigences légales concernant la vie privée, le traitement des données et la sécurité ?** ◯ Oui ◯ Non
- Etes-vous conscient(e) des cybermenaces et des vulnérabilités sur vos réseaux ? ◯ Oui ◯ Non

2. Elaboration d'une politique de sécurité et d'un code de bonne conduite

- Avez-vous mis en place une politique écrite en matière de sécurité de votre système informatique et y avez-vous sensibilisé les utilisateurs ? ◯ Oui ◯ Non
- **Appliquez-vous des procédures pour l'arrivée et le départ d'utilisateurs (personnel, stagiaires, etc.) ?** ◯ Oui ◯ Non
- **Avez-vous décrit les rôles et les responsabilités en matière de sécurité (physique, personnel et ICT) ?** ◯ Oui ◯ Non
- **Avez-vous diffusé en interne un code de bonne conduite sur l'utilisation des ressources informatiques ?** ◯ Oui ◯ Non
- Planifiez-vous et exécutez-vous des audits de sécurité ? ◯ Oui ◯ Non

3. Sensibilisation du personnel au risque Cyber

- Encouragez-vous les utilisateurs à respecter votre code de bonne conduite y compris la gestion des mots de passe? ◯ Oui ◯ Non
- **Rappelez-vous régulièrement aux utilisateurs l'importance de rester vigilants par rapport à la sécurité informatique ?** ◯ Oui ◯ Non
- **Rappelez-vous régulièrement aux utilisateurs que les informations doivent être considérées comme sensibles et traitées dans le respect des règles de protection de la vie privée ?** ◯ Oui ◯ Non
- **Informez-vous les utilisateurs sur la façon de reconnaître le phishing (fraude par e-mail) et la réaction à adopter ?** ◯ Oui ◯ Non
- **Avez-vous informé les collaborateurs du service Comptabilité du phénomène de « fraude au CEO » et prévoyez-vous des procédures de contrôle dans le cadre de l'exécution des paiements ?** ◯ Oui ◯ Non

4. Gestion des ressources informatiques importantes

- Tenez-vous un inventaire de l'ensemble des équipements ICT et des licences de logiciels ? ◯ Oui ◯ Non
- Maintenez-vous une carte détaillée et actualisée de tous vos réseaux et interconnexions ? ◯ Oui ◯ Non

5. Mise à jour des programmes

- **Installez-vous régulièrement les mises à jour (Patch) des logiciels dont vous disposez sur les postes de travail, les appareils mobiles, les serveurs et les composants de réseau...) ?** ◯ Oui ◯ Non
- Procédez-vous aux mises à jour de sécurité de tous les logiciels dans les plus brefs délais ? ◯ Oui ◯ Non
- Avez-vous automatisé le processus de mise à jour et auditez-vous son efficacité ? ◯ Oui ◯ Non

6. Installation d'une protection antivirus

- **Avez-vous installé un logiciel antivirus sur tous les postes de travail et les serveurs ?** ◯ Oui ◯ Non
- **Votre antivirus est-il mis à jour au moins hebdomadairement ?** ◯ Oui ◯ Non
- Les mises à jour de votre antivirus se font-elles automatiquement ? ◯ Oui ◯ Non
- Les utilisateurs savent-ils comment l'antivirus alerte en cas d'infection virale ? ◯ Oui ◯ Non
- **Disposez-vous d'un pare-feu qui protège votre système et qui est mis à jour au moins hebdomadairement ?** ◯ Oui ◯ Non

7. Sauvegarde de toutes les informations

- **Effectuez-vous des sauvegardes hebdomadairement ?** ◯ Oui ◯ Non
- **Les sauvegardes sont-elles testées au moins annuellement ?** ◯ Oui ◯ Non
- Hébergez-vous des solutions de sauvegarde sur vos propres serveurs ? ◯ Oui ◯ Non
- Utilisez-vous des solutions de stockage dans le cloud ? ◯ Oui ◯ Non
- Les sauvegardes sont-elles stockées sur un autre site que le système informatique ? ◯ Oui ◯ Non
- Si oui, sont-elles externalisées auprès d'une société spécialisée ? ◯ Oui ◯ Non
- Procédez-vous à l'encryptage des données ? ◯ Oui ◯ Non

  Si oui, quelles données ?

8. Gestion de l'accès aux ordinateurs et au réseau

- **Imposez-vous l'utilisation de mots de passe personnels et robustes (avec mélange de chiffres, caractères spéciaux, majuscules…) d'au moins 6 caractères ?** ◯ Oui ◯ Non
- **Modifiez-vous ces mots de passe au moins trimestriellement et de façon automatique (ou imposée par le système) ?** ◯ Oui ◯ Non
- **Les mots de passe sont-ils modifiés en cas de soupçon de piratage ?** ◯ Oui ◯ Non
- **Changez-vous tous les mots de passe par défaut ?** ◯ Oui ◯ Non
- Quelqu'un dispose-t-il de privilèges d'administrateur pour les tâches quotidiennes ? ◯ Oui ◯ Non
- **Maintenez-vous une liste limitée et actualisée des comptes d'administrateur du système ?** ◯ Oui ◯ Non
- **Utilisez-vous uniquement des comptes individuels ?** ◯ Oui ◯ Non
- **Désactivez-vous immédiatement les comptes non utilisés ?** ◯ Oui ◯ Non
- Les droits et les privilèges sont-ils gérés par groupes d'utilisateurs ? ◯ Oui ◯ Non
- Les droits d'accès du personnel sont-ils déterminés en fonction du niveau de responsabilité de l'utilisateur ? ◯ Oui ◯ Non
- Appliquez-vous une politique d'accès spécifique au système informatique pour les sous-traitants ou fournisseurs ? ◯ Oui ◯ Non

9. Sécurisation des postes de travail et des appareils mobiles

- **Les postes de travail et les appareils mobiles non utilisés sont-ils verrouillés automatiquement ?** ◯ Oui ◯ Non
- Les ordinateurs portables, les tablettes et les smartphones sont-ils parfois laissés sans surveillance ? ◯ Oui ◯ Non
- **Désactivez-vous la fonction « Autorun » des médias externes ?** ◯ Oui ◯ Non
- Stockez-vous ou copiez-vous toutes les données sur un serveur ou un NAS (Network Area Storage) ? ◯ Oui ◯ Non
- Autorisez-vous l'emploi de matériel privé (PC, GSM…) ? ◯ Oui ◯ Non

10. Sécurisation des serveurs et des composants de réseau

- **Les locaux de l'entreprise sont-ils sécurisés de manière à empêcher d'atteindre le(s) serveur(s) ?** ◯ Oui ◯ Non
- **Le réseau public Wifi est-il séparé du réseau d'entreprise ?** ◯ Oui ◯ Non
- Protégez-vous le wifi par un cryptage WPA2 ? ◯ Oui ◯ Non
- Fermez-vous les ports et les services non utilisés ? ◯ Oui ◯ Non
- **Evitez-vous la connexion à distance aux serveurs (protocole RPC) ?** ◯ Oui ◯ Non
- Utilisez-vous des applications et des protocoles sécurisés ? ◯ Oui ◯ Non
- Les journaux de sécurité sur les serveurs et les pare-feux sont-ils conservés pendant une période d'au moins 1 mois ? ◯ Oui ◯ Non

11. Sécurisation des accès à distance

- L'accès à distance est-il fermé automatiquement en cas d'inactivité pendant un certain temps ? ◯ Oui ◯ Non
- **Limitez-vous l'accès à distance à ce qui est strictement nécessaire ?** ◯ Oui ◯ Non
- Toutes les connexions au réseau d'entreprise sont-elles sécurisées et cryptées ? ◯ Oui ◯ Non
- **Sécurisez-vous les connexions au système informatique via internet (PC portables, GSM, tablettes…) par l'utilisation de l'outil VPN ?** ◯ Oui ◯ Non

12. Mise à disposition d'un plan de la continuité des activités & d'un plan de gestion des incidents

- **Disposez-vous d'un plan de gestion des incidents afin de répondre à un incident ?** ◯ Oui ◯ Non
- Diffusez-vous et actualisez-vous les informations sur le point de contact (contacts internes et externes, direction et contacts techniques…) ? ◯ Oui ◯ Non
- **Signalez-vous tous les incidents au management ?** ◯ Oui ◯ Non
- Avez-vous rédigé, testé et mis à jour un plan de continuité en cas de cyberattaque ? ◯ Oui ◯ Non
- Avez-vous déjà notifié un événement tombant sous le champ d'application du RGPD ? ◯ Oui ◯ Non
- Avez-vous déjà été victime d'une cyberattaque ? ◯ Oui ◯ Non

  Si oui, de quelle nature ?

- A partir de quelle durée d'interruption de votre système informatique vos activités subiront-elles un impact notable ?

  ◯ moins de 12 h ◯ entre 12 et 24 h ◯ de 1 à 2 jours ◯ de 2 à 5 jours ◯ plus de 5 jours

13. Type de données utilisées

- Utilisez-vous des données personnelles de particuliers (autres que celles de vos employés ou agents) ? ◯ Oui ◯ Non
- Est-il possible de faire des paiements en ligne sur le site web de l'entreprise ? ◯ Oui ◯ Non

Fait à le

Nom et fonction de la personne de contact