Mesures de sécurité : les questions à se poser pour une bonne hygiène informatique

Afin de répondre à ces questions, vous devez :

- **Recenser et documenter les logiciels utilisés** (nom du logiciel métier, Word, Excel, etc.) et leurs versions actuelles.
- **Identifier et évaluer les menaces potentielles** et leurs impacts sur la vie privée des personnes concernées en réalisant une analyse de risques approfondie.
- **Prévoir les mesures de sécurité adaptées à ces menaces**, y compris les modalités de sauvegarde et les lieux d'hébergement sécurisés. Ces mesures doivent être régulièrement mises à jour pour rester efficaces face aux nouvelles menaces.

<u>Authentification des utilisateurs</u> :

- **Avez-vous défini un identifiant (login) unique** pour chaque utilisateur afin de garantir une traçabilité précise des actions ?
- **Exigez-vous des utilisateurs des mots de passe robustes**, comprenant un minimum de 12 caractères, des lettres majuscules et minuscules, des chiffres et des caractères spéciaux ?
- **Avez-vous mis en place une politique de renouvellement des mots de passe** obligeant les utilisateurs à changer leur mot de passe après enrôlement et à intervalles réguliers (tous les 3 mois par exemple) ?
- **Utilisez-vous une authentification à deux facteurs (2FA)** pour renforcer la sécurité des comptes utilisateurs ?
- **Avez-vous établi une procédure** en cas de perte des identifiants ?
- **Assurez-vous la sensibilisation et la formation des utilisateurs** sur les bonnes pratiques en matière de gestion des mots de passe et de sécurité des comptes ?

<u>Gestion des privilèges d'accès</u> :

- **Avez-vous défini différents profils d'habilitation** (basés sur le principe du « *moindre privilège* ») en fonction des rôles et responsabilités des personnes ayant accès aux informations ?
- **Supprimez-vous régulièrement les permissions d'accès obsolètes** pour éviter tout accès non autorisé aux informations ?
- **Avez-vous rédigé et communiqué une charte informatique** à tous les utilisateurs du Système d'Information (salariés, stagiaires, prestataires, etc.), détaillant les bonnes pratiques et les obligations en matière de sécurité des données ?
- **Organisez-vous des formations régulières** pour sensibiliser les employés à la sécurité des données et à l'utilisation des systèmes d'information ?
- **Effectuez-vous des audits périodiques des privilèges d'accès** pour garantir leur conformité avec la ou les politique(s) de sécurité de votre organisme ?

<u>Sécurisation des postes de travail des utilisateurs</u> :

- **Limitez-vous le nombre de tentatives d'accès à un compte** ?
- **Avez-vous installé un pare-feu logiciel** ?
- **Utilisez-vous des antivirus régulièrement mis à jour** ?
- **Installez-vous sans délai les mises à jour critiques (correctifs de sécurité)** pour corriger les vulnérabilités des systèmes d'exploitation et des logiciels ?
- **Chiffrez-vous les données** stockées sur les postes de travail, y compris les unités de stockage (disques durs externes, USB, etc.) ?
- **Utilisez-vous un dispositif de verrouillage automatique de session** après un bref temps d'inactivité pour éviter les accès non autorisés ?
- **Effectuez-vous des audits réguliers** des postes de travail pour vérifier la conformité aux politiques de sécurité et identifier les éventuelles vulnérabilités ?
- **Avez-vous instauré des procédures de sauvegarde régulières** des données importantes stockées sur les postes de travail pour prévenir les pertes de données en cas de panne ou d'attaque ?
- **Avez-vous sensibilisé et formé les utilisateurs** à l'importance de la sécurisation des données sur les appareils et supports nomades ?
- **Utilisez-vous des solutions de gestion des appareils mobiles (MDM)** afin de renforcer la sécurité et la conformité des appareils nomades utilisés par les employés?

<u>Continuité de l'activité de votre organisme</u> :

- **Avez-vous prévu des moyens de sécurité** pour vos sauvegardes effectuées sur un site extérieur, garantissant ainsi la disponibilité des données en cas de sinistre majeur ?
- **Avez-vous éventuellement mis en place un plan de continuité d'activité** détaillant les procédures à suivre en cas de perturbation majeure, afin de minimiser les interruptions et de maintenir le fonctionnement des services critiques ?
- **Avez-vous élaboré un plan de reprise d'activité** pour restaurer rapidement les systèmes d'information et les données après un incident ?
- **Testez-vous régulièrement ce(s) plan(s)** pour vous assurer de son (leur) efficacité et pour identifier d'éventuels points d'amélioration ?
- **Organisez-vous des exercices et des simulations** pour préparer votre personnel à réagir efficacement en cas de crise ?

<u>Encadrement des opérations de maintenance</u> :

- **Enregistrez-vous les interventions de maintenance** dans une main courante pour assurer une traçabilité complète des actions effectuées ?
- **Accompagnez-vous et supervisez-vous** toute intervention des prestataires pour garantir le respect des procédures de sécurité et de confidentialité ?
- **Effacez-vous les données de tout matériel** *(blanchir le matériel)* avant sa mise au rebut pour prévenir tout risque de récupération de données ?
- **Informez-vous les utilisateurs** avant toute intervention sur leur poste de travail ?
- **Exigez-vous des prestataires qu'ils respectent les normes de sécurité en vigueur** et les clauses de confidentialité des données ?

Gestion des accès au système d'information (SI) de votre organisme et gestion des incidents :

- **Avez-vous mis en place un système de journalisation** des accès ?
- **Avez-vous informé les utilisateurs** de la mise en place de ce système de journalisation ?
- **Avez-vous protégé les équipements de journalisation et les informations journalisées** contre les accès non autorisés et les altérations ?
- **Disposez-vous d'une procédure de gestion des incidents de sécurité** incluant la détection, l'analyse et la résolution rapide des incidents ?

Protection de l'accès aux serveurs, équipements de sécurité et autres unités de stockage :

- **Avez-vous installé des portes verrouillées** pour contrôler l'accès physique aux serveurs, équipements de sécurité et autres unités de stockage ?
- **Avez-vous installé des alarmes anti-intrusion** pour détecter et prévenir toute tentative d'accès non autorisé ?
- **Vérifiez-vous périodiquement les systèmes de sécurité** pour vous assurer de leur bon fonctionnement et de leur efficacité ?
- **Utilisez-vous des dispositifs de surveillance vidéo** pour surveiller et enregistrer les zones sensibles (exemple : salle serveurs) ?
- **Effectuez-vous des audits de sécurité réguliers** pour identifier et corriger les éventuelles vulnérabilités dans vos systèmes de protection ?

Protection du réseau informatique interne :

- **Avez-vous limité les flux réseau au strict nécessaire** ?
- **Avez-vous sécurisé les accès distants des appareils informatiques nomades par VPN** pour garantir la confidentialité et l'intégrité des communications ?
- **Utilisez-vous le protocole TLS avec une clé d'au moins 128 bits** pour protéger les services web et garantir des connexions sécurisées ?
- **Avez-vous mis en œuvre le(s) protocole(s) de sécurité** (WEP2, WEP3, etc.) **pour les réseaux Wifi** ?
- **Chiffrez-vous toutes vos données** (au repos et en mouvement) ?
- **Avez-vous mis en place une politique de gestion des accès Wifi** ?
- **Utilisez-vous des solutions de détection et de prévention des intrusions** (IDS/IPS) ?
- **Avez-vous mis en place des politiques de segmentation du réseau** pour isoler les systèmes et limiter les impacts en cas de compromission d'une partie du réseau ?

Sécurisation des serveurs et des applications :

- **Avez-vous adopté une politique de mot de passe administrateur rigoureuse** ?
- **Avez-vous installé un pare-feu logiciel** sur chaque serveur ?
- **Utilisez-vous des antivirus régulièrement mis à jour** ?
- **Installez-vous sans délai les mises à jour critiques (correctifs de sécurité)** pour corriger les vulnérabilités des systèmes d'exploitation et des logiciels ?
- **Chiffrez-vous les données** stockées sur les serveurs et les applications pour protéger la confidentialité des informations ?
- **Effectuez-vous des audits de sécurité réguliers** pour identifier et corriger les éventuelles vulnérabilités dans vos serveurs et applications ?
- **Avez-vous mis en place des politiques de mise à jour et de sauvegarde régulières** des données stockées sur les serveurs et les applications pour éviter les pertes en cas de défaillance ?
- **Formez-vous régulièrement vos administrateurs système** aux meilleures pratiques en matière de sécurité des serveurs et des applications ?
- **Avez-vous mis en place des politiques de mise à jour et de sauvegarde régulières** des équipements de sécurité ?

Gestion des archives :

- **Avez-vous mis en œuvre des modalités d'accès spécifiques** (habilitations restreintes, bases de données séparées, etc.) pour protéger les données archivées et en garantir la confidentialité ?
- **Détruisez-vous les archives de manière sécurisée**, en suivant des procédures strictes pour éviter toute récupération non autorisée des données ?
- **Disposez-vous d'un plan de conservation des archives** détaillant les durées de conservation des différentes catégories de données et les conditions de leur destruction ?
- **Avez-vous mis en place des politiques de gestion des archives** pour garantir l'intégrité, la confidentialité et la disponibilité des données archivées ?

Échanges avec les autres organismes :

- **Chiffrez-vous les données sensibles avant leur envoi par tout canal de communication** pour garantir leur confidentialité et leur intégrité durant le transit ?
- **Transmettez-vous le code secret de déchiffrement** dans un envoi distinct et via un canal différent pour renforcer la sécurité des échanges ?
- **Avez-vous mis en place des politiques de gestion des échanges de données** ?
- **Sensibilisez-vous et formez-vous régulièrement les employés** aux bonnes pratiques de sécurité concernant les échanges de données avec des organismes externes ?
- **Avez-vous établi des accords de confidentialité et de traitement des données** avec les organismes partenaires pour garantir le respect des obligations légales et des bonnes pratiques en matière de protection des données ?

Relations avec les prestataires informatiques (si concerné) :

- **Avez-vous prévu une clause spécifique de confidentialité dans tous les contrats de sous-traitance** ?
- **Avez-vous vérifié que les garanties annoncées par les prestataires étaient effectives** (audits de sécurité, visites sur site, contrôles réguliers, etc.) ?
- **Avez-vous prévu des conditions de restitution et /ou de destruction des données** dans les contrats de sous-traitance ?
- **Établissez-vous des rapports périodiques** avec les prestataires pour suivre les performances, les incidents de sécurité et les mesures correctives mises en œuvre ?