

Checklist Cybersécurité

PROTECTION RÉSEAUX

- Mettre à jour régulièrement les systèmes d'exploitation (Windows, macOS, Linux) et les logiciels pour corriger les failles de sécurité.
- Utiliser un anti-virus de qualité
- Configurer un pare-feu
- Segmenter les réseaux

GESTION DES ACCÈS

- Utiliser des mots de passe forts et les changer régulièrement
- Mettre en place l'authentification à deux facteurs sur les comptes critiques
- Limiter les accès au réseau et aux données sensibles selon le principe du moindre privilège

FORMATIONS

- Former régulièrement les agents et les élus concernés par les données
- Simuler des attaques pour s'entraîner
- Mettre en place une politique de sécurité informatique et faire signer la charte par les élus et les agents

SAUVEGARDES

- Effectuer des sauvegardes régulières des données importantes
- Stocker les sauvegardes dans un endroit sécurisé (cloud, hors site) et les tester
- Mettre en place un plan de reprise après sinistre et le tester pour l'améliorer avec les données terrain

COMMUNICATION

- Utiliser des connexions sécurisée (https, VPN, etc.) pour les données
- Crypter les email contenant des informations sensibles ou utiliser des plateformes sécurisées
- Vérifier les adresses emails avant de transférer des paiements ou des infos

SURVEILLANCE

- Surveiller les activités suspectes avec des outils (IDS/IPS)
- Elaborer un plan d'intervention en cas d'incident pour réagir efficacement
- Maintenir un contact avec des experts en cybersécurité pour avoir de l'aide

Checklist Cybersécurité

CONFORMITÉ

- Veiller à la conformité RGPD en protégeant les données personnelles
- Mettre en place des audits réguliers de conformité et des pratiques de sécurité
- Sensibiliser sur la gestion des données sensibles et de leur destruction

SÉCURITÉ MOBILES

- Imposer l'utilisation de dispositifs de sécurité sur les téléphones
- Restreindre l'accès aux réseaux municipaux depuis les appareils perso
- Bloquer l'accès aux applications non nécessaires sur les mobiles

SOUS-TRAITANTS

- Evaluer la cybersécurité des partenaires et prestataires
- Signer des accords de confidentialité et de sécurité pour garantir le respect des normes

PROTECTION ATTAQUES

- Implémenter une protection contre les ransomwares et autres logiciels malveillants
- Utiliser des solutions de détection des intrusions et bloquer les accès non autorisés
- Vérifier régulièrement les accès à distance