Qualités organisationnelles - BONNES PRATIQUES

Sécurisation des données et mise en conformité des processus

- Installer des pare-feux avancés et des solutions EDR (système de surveillance et de détection des activités malveillantes);
- Former en continu les équipes sur les bonnes pratiques en matière de cybersécurité et relativement aux obligations de conformité;
- Intégrer des solutions de cybersécurité avancées;
- Instaurer une politique de gouvernance pour la gestion des données;
- Réaliser des audits internes et/ou externes (cybersécurité et Loi 25);
- Respecter les réglementations applicables (Loi 25);
- Documenter les incidents et les mesures correctives appliquées.

Numérisation des processus de travail et intégration des outils numériques

- Cartographier les processus de travail afin d'avoir une vision concrète et commune des étapes réalisées;
- Numériser les processus comptables (feuilles de temps, paie, facturation, etc.);
- Passer à une gestion documentaire numérique, incluant la signature de documents (SharePoint, OneDrive, Adobe, etc.);
- Utiliser des tablettes pour numériser les tâches administratives reliées aux aides à domicile (gestion de l'horaire, annulations, communication, etc.);
- Numériser les activités des ressources humaines (dotation, vacances, etc.);
- Intégrer (interconnecter) les logiciels des différents départements afin de centraliser la gestion des données;
- Bénéficier d'un accompagnement en transformation numérique.

Développement des compétences numériques de l'équipe

- Suivi de mise en œuvre des apprentissages réalisés dans les formations récentes;
- Mettre en place un plan de formation selon le poste;
- Assurer une assistance technique en ligne (possibilité de générer une FAQ) ou guider les employé·es vers le support proposé par les éditeurs de logiciels;
- Désigner les employé·es responsables de l'intégration des nouveaux outils numériques ainsi que le suivi de l'adoption auprès des collègues (super utilisateurs);
- Diversifier les employés responsables du bon fonctionnement des outils numériques (Microsoft 365, Maya, Acomba, etc.) selon le niveau d'aisance et la pertinence du poste.

Maturité numérique organisationnelle

- Évaluer régulièrement les besoins des équipes pour vous assurer que les outils en place répondent aux usages réels;
- Effectuer de la veille technologique active pour rester à l'affût des nouvelles solutions pertinentes pour l'organisation;
- Tester les outils avant leur adoption afin de valider leur utilité et leur compatibilité avec l'environnement existant;
- Offrir de la formation continue aux employé·es pour garantir une utilisation optimale et évolutive des outils disponibles;
- Mettre en place un registre des outils numériques, incluant la liste de l'ensemble des outils disponibles, les fonctionnalités utilisées et celles non explorées, les irritants et les solutions expérimentées;
- Toujours explorer les fonctionnalités des outils disponibles avant de songer à acheter de nouveaux logiciels ou à changer.

Cybersécurité

- **Gouvernance et politiques :**
  - Rédiger et diffuser une politique de sécurité informatique claire;
  - Définir les rôles et responsabilités en matière de cybersécurité;
  - Mettre en place un Plan de Gestion des Incidents (PGI);
  - Maintenir un registre des actifs informatifs.
- **Mesures de protection techniques :**
  - Installer et maintenir à jour : antivirus / anti-malware / pare-feu / filtrage Web;
  - Activer l'authentification à deux facteurs (MFA);
  - Appliquer des mises à jour de sécurité automatiques;
  - Restreindre les accès selon le principe du moindre privilège;
  - Sécuriser les connexions à distance (VPN, chiffrement, etc.);
  - Surveiller les journaux d'activité système (SIEM si possible);
- **Sauvegarde et continuité des activités :**
  - Effectuer des sauvegardes régulières (quotidiennes si possible);
  - Tester les restaurations de données pour vérifier la fiabilité;
  - Stocker les sauvegardes dans un lieu sécurisé (hors site ou infonuagiques chiffrées);
  - Élaborer un Plan de Reprise des Activités (PRA) et un Plan de continuité (PCA);
- **Sensibilisation et formation :**
  - Organiser des simulations d'hameçonnage;
  - Mettre à disposition des guides internes ou affiches de bonnes pratiques;
  - Sensibiliser aux risques d'ingénierie sociale;
  - Communiquer régulièrement sur les nouveaux risques (rançongiciels, failles récentes).

Revision #2
Created 29 July 2025 01:32:09 by Admin
Updated 14 October 2025 19:08:57 by Admin