Usage des Outils Informatiques

1. Objectifs et Champ d'Application

Ce document vise à encadrer l'utilisation des moyens informatiques et des outils numériques mis à disposition par KNG Enterprise. Il définit les règles d'usage, de sécurité et de responsabilité applicables à tous les utilisateurs (employés, stagiaires, prestataires).

2. Moyens Informatiques Concernés

Les moyens informatiques incluent :

- Les ordinateurs, portables, tablettes, smartphones, et autres postes de travail attribués.
- L'accès au réseau interne, à Internet et à la messagerie électronique professionnelle.
- Les logiciels fournis par KNG Enterprise.
- Les périphériques (imprimantes, clés USB, supports amovibles).

3. Règles Générales d'Usage

- Usage professionnel prioritaire : Les ressources informatiques sont réservées à un usage professionnel, liés aux missions confiées.
    - Un usage personnel mineur et raisonnable est toléré si cela ne gêne pas la bonne marche du service ni la sécurité du système d'information.
- Confidentialité : Il est interdit de communiquer à l'extérieur de l'entreprise toute information sensible ou confidentielle accessible via les outils informatiques.
- Protection des accès :
    - Chaque utilisateur doit protéger l'accès à son poste de travail via un mot de passe robuste, strictement personnel et renouvelé régulièrement.
    - Les identifiants et mots de passe ne doivent en aucun cas être partagés.
- Respect des droits d'auteur : Toute installation de logiciel ou copie de fichier doit être préalablement validée par le service IT. Il est strictement interdit d'installer ou d'utiliser des logiciels piratés.
- Sécurité :
    - Ne jamais ouvrir de courriels, liens ou pièces jointes suspects.

        - Signaler sans délai au service IT tout incident, anomalie ou tentative d’accès illicite.
        - Utiliser uniquement des supports amovibles (clé USB, disque dur externe) approuvés par le service IT après analyse antivirus.
- Matériel :
    - Ne pas modifier la configuration des postes, ni démonter ou réparer le matériel sans autorisation.
    - À la fin du contrat, restituer tout matériel et effacer ses fichiers privés conformément aux règles internes.

4. Accès et Traçabilité

- Les accès aux outils et ressources informatiques sont enregistrés ; des contrôles et audits peuvent être réalisés par l’entreprise dans un cadre légal pour assurer la sécurité et le respect des règles.

5. Chartes Spécifiques et Sanctions

- Le non-respect de ce guide expose l’utilisateur à des sanctions disciplinaires pouvant aller jusqu’au licenciement, conformément au règlement intérieur de KNG Enterprise.
- Ce guide complète le règlement intérieur et la charte informatique générale qui peuvent contenir des exigences complémentaires.

6. Bonnes Pratiques à Rappeler

1. Vérifiez toujours l’expéditeur avant d’ouvrir une pièce jointe.
2. Verrouillez votre session à chaque absence, même brève.
3. Sauvegardez vos documents sur les espaces réseau sécurisés.
4. Ne connectez pas de périphérique personnel sans accord IT.
5. Signalez toute perte, vol ou défaillance de matériel ou d’accès.

L’adoption de ce cadre contribue à la sécurité collective, à la protection des données et à la performance informatique de KNG Enterprise.

2. Sécurité informatique

Ce chapitre détaille les principes et bonnes pratiques à suivre chez KNG Enterprise pour assurer la sécurité informatique, protéger les actifs numériques, et se conformer aux réglementations (RGPD, NIS2, etc.). Un système d'information sécurisé est essentiel pour éviter les cyberattaques, limiter les fuites de données, et maintenir la continuité des activités.

2.1 Principes de la sécurité informatique

- Confidentialité : Protéger les informations sensibles contre tout accès non autorisé.
- Intégrité : Garantir que les données et systèmes ne sont ni altérés ni corrompus par accident ou action malveillante.
- Disponibilité : Assurer l'accès aux ressources informatiques et aux données pour les utilisateurs habilités quand ils en ont besoin.
- Traçabilité : Enregistrer et suivre les accès, modifications et incidents sur les systèmes et données.

2.2 Politique de sécurité informatique (PSSI)

KNG Enterprise dispose d'une Politique de Sécurité des Systèmes d'Information, qui repose sur les points suivants :

- Définition du périmètre : Identification des actifs à protéger (données, serveurs, réseaux, applications, terminaux).
- Analyse des risques : Évaluation des menaces, vulnérabilités, et impacts potentiels via audits réguliers.
- Règles, mesures et procédures : Formalisation de règles internes (accès, mots de passe, sauvegardes, chiffrement, etc.) et des procédures à suivre en cas d'incident ou de suspicion d'incident.
- Contrôle des accès : Limitation de l'accès aux données sensibles aux seules personnes autorisées ; authentification forte recommandée (mots de passe complexes, double facteur).
- Gestion des incidents : Mise en place de procédures de détection et réponse rapide aux incidents (virus, ransomware, fuite, etc.), ainsi que la tenue d'un registre des incidents.
- Continuité d'activité : Prévoir la sauvegarde régulière, le plan de reprise informatique, et les solutions de secours (redondance, plan B) pour maintenir le service en cas de crise.

2.3 Bonnes pratiques pour tous les utilisateurs

- Ne jamais ouvrir de liens ou pièces jointes suspects dans les courriels ou messageries instantanées.
- Verrouiller son poste à chaque absence, même pour un court instant.
- Effectuer des sauvegardes régulières sur les espaces réseau sécurisés ou clouds validés ; ne pas conserver d'informations importantes sur le poste local.
- Utiliser des mots de passe robustes et uniques pour chaque application ou outil.
- Signaler rapidement toute anomalie, tentative d'intrusion, ou incident au service IT.
- Limiter l'utilisation d'outils personnels ou non validés pour le travail (USB, logiciels, etc.).
- Activer le pare-feu et les protections antivirus.
- Utiliser un VPN lors d'un accès distant ou en télétravail pour sécuriser les flux de données.
- Respecter la confidentialité et la non-divulgation des informations professionnelles et personnelles.
- Participer aux formations et campagnes de sensibilisation à la cybersécurité.

2.4 Conformité réglementaire

KNG Enterprise applique et met à jour ses procédures pour répondre aux obligations RGPD, NIS2, ISO 27001 et recommandations de l'ANSSI. Ceci inclut la protection des données personnelles, la gestion des droits d'accès, la traçabilité, et la réactivité face aux incidents. Des audits et contrôles internes sont régulièrement réalisés.

2.5 Rôles et responsabilités

- Responsable informatique : pilote la politique de sécurité, assure la veille technologique et le suivi des incidents.
- Service IT : maintenance des systèmes, déploiement des protections, gestion des utilisateurs, support et formation continue.
- Utilisateurs : respectent toutes les règles, signalent tout dysfonctionnement et participent à la sensibilisation.

2.6 Sanctions et sensibilisation

- Toute violation des règles de sécurité peut entraîner des sanctions disciplinaires (avertissement, suspension, licenciement).

- Des sessions régulières de formation et de sensibilisation sont obligatoires pour tous les personnels.

Résumé pratique :

- Sécurisation = Confidentialité + Intégrité + Disponibilité + Traçabilité
- Audit, contrôle des accès, formation, vigilance et respect permanent sont les clés d'une sécurité informatique efficace.

3. Politique de mot de passe

La politique de mot de passe de KNG Enterprise vise à protéger les données et systèmes de l'entreprise contre les accès non autorisés, conformément aux exigences règlementaires comme le RGPD et la directive NIS2. Cette politique s'applique à tous les utilisateurs ayant accès aux ressources informatiques de l'entreprise.

1. Objectifs de la politique

- Renforcer la protection des informations sensibles contre les intrusions et les fuites.
- Limiter les risques d'attaques par compromission de mots de passe (phishing, force brute, etc.).
- Répondre aux obligations réglementaires en matière de cybersécurité et de conformité.

2. Règles de création des mots de passe

- Longueur minimale : au moins 12 caractères (idéalement 14).
- Complexité : Doit contenir une combinaison de majuscules, minuscules, chiffres et caractères spéciaux.
- Interdictions : Pas de mot de passe basé sur des données personnelles (nom, date de naissance, nom de l'entreprise) ou des mots du dictionnaire.
- Unicité : Un mot de passe doit être unique pour chaque compte ou application ; la réutilisation est strictement interdite.
- Historique : Un utilisateur ne peut pas réutiliser ses 5 anciens mots de passe.

3. Gestion et renouvellement des mots de passe

- Renouvellement automatique : Les mots de passe doivent être changés tous les 180 jours (ou en cas de soupçon de compromission).
- Modification immédiate : En cas de doute ou d'incident suspecté, l'utilisateur doit changer son mot de passe sans délai.

- Changement des mots de passe par défaut : Tous les mots de passe par défaut (fournis par le constructeur ou lors de la première utilisation) doivent être remplacés immédiatement.

4. Stockage et partage

- Stockage sécurisé : Ne jamais écrire ou stocker un mot de passe en clair (post-it, document texte non sécurisé). Utiliser uniquement des gestionnaires de mots de passe validés par l'IT.
- Non-partage : Les mots de passe sont strictement individuels et ne doivent jamais être partagés, transmis ou communiqués, même temporairement, à des collègues ou à des prestataires.

5. Protection des accès

- Authentification multifactorielle (MFA) : Elle doit être activée dès que l'outil ou l'application le permet.
- Verrouillage de compte : Après un maximum de 5 tentatives erronées, l'accès au compte est verrouillé pour une durée de 15 minutes (ou selon la politique IT).

6. Bonnes pratiques et sensibilisation

- Assister aux sessions de sensibilisation à la sécurité informatique organisées par KNG Enterprise.
- Toujours vérifier l'origine des demandes de « réinitialisation de mot de passe », pour éviter le phishing.
- Signaler sans délai auprès du service IT toute anomalie ou suspicion de compromission d'identifiants.

7. Contrôles et sanctions

- Des audits réguliers sont effectués pour vérifier la conformité à la politique de mot de passe.
- Tout manquement (mot de passe faible, partage, stockage non sécurisé) pourra faire l'objet de sanctions disciplinaires conformément au règlement intérieur.

Note : Cette politique doit être lue, comprise et signée par chaque utilisateur. Elle est révisée annuellement ou en cas d'évolution réglementaire ou technologique.

2.6 Sanctions et sensibilisation

- Toute violation des règles de sécurité peut entraîner des sanctions disciplinaires (avertissement, suspension, licenciement).
- Des sessions régulières de formation et de sensibilisation sont obligatoires pour tous les personnels.

Résumé pratique :

- Sécurisation = Confidentialité + Intégrité + Disponibilité + Traçabilité
- Audit, contrôle des accès, formation, vigilance et respect permanent sont les clés d’une sécurité informatique efficace.