

Engagement de conformité et de bon usage

Comptes à privilèges

Engagement de conformité et de bon usage relatif à l'utilisation des technologies de l'information et de communication du G.I.E. GPM par des utilisateurs disposant de comptes à privilèges

Reconnais que :

Le présent engagement vient enrichir l'annexe du règlement intérieur : « **Charte d'utilisation des Technologies de l'Information et de Communication du G.I.E. GPM** » qui continue de s'appliquer pleinement.

Cette annexe, consultable sur l'Intranet spécifie notamment que :

« Les administrateurs sont tenus au secret professionnel et ne doivent divulguer aucune des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne peuvent être contraints de le faire. »

Ainsi, [...], les administrateurs ne procéderont, à leur initiative ou sur ordre hiérarchique, à aucune exploitation d'un document identifié formellement comme personnel.

Par ailleurs, les administrateurs de la direction des systèmes d'information sont tenus à une responsabilité et à des obligations renforcées par rapport à celle des autres utilisateurs notamment en matière de confidentialité et d'intégrité dans l'exercice de leur métier.

En revanche, si un fichier est identifié comme étant personnel, l'employeur ne peut y avoir accès « qu'en présence du salarié ou si celui-ci a été dûment appelé, ou en cas de risque ou événement particulier » (Cass. soc. 17 mai 2005 n° 03-40.017 ; Cass. soc. 17 juin 2009 n° 08-40.274 : N-VIII- 6260 s.). Le collaborateur ne peut pas s'opposer à un tel accès si ces conditions ont été respectées. »

En conséquence, je m'engage à :

- respecter strictement les obligations légales en termes d'accès aux informations confidentielles et données à caractère personnel au sens du règlement européen sur la protection des données ainsi que les données relevant du secret professionnel,
- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions,
- ne jamais transmettre mes identifiants à autrui,



- ne pas ouvrir de boîte aux lettres ou de compte informatique d'un utilisateur de l'entreprise sans sa présence ou sans son accord préalable,
- ne pas ouvrir* de fichier ou répertoire dont la désignation indique que son contenu est privé / personnel,
- ne jamais réaliser d'assistance à distance** sur un poste d'un utilisateur sans l'accord préalable de ce dernier,
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse du système d'information,
- prendre toutes précautions conformes à la politique de sécurité du système d'information pour préserver la sécurité du système d'information,
- d'utiliser des moyens de communication sécurisés pour transférer des données,
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.
- de répondre favorablement, et dans les délais les plus courts, aux consignes de surveillance, de recueil d'information et d'audit émis par le RSSI ;
- de traiter en priorité toute violation des règles SSI et tout incident de sécurité qu'il est serait amené à constater, puis d'informer sans délai le RSSI selon la procédure prévue par la chaîne fonctionnelle de sécurité, et d'appliquer sans délai les instructions du RSSI pour le traitement de l'incident.

En particulier, je m'interdis de :

- installer ou faire procéder à l'installation de logiciels :
 - pour lesquels le Groupe n'aurait pas acquis de licence d'exploitation,
 - n'ayant pas de rapport direct avec l'activité professionnelle,
 - mettant en péril l'intégrité des données et des systèmes du Groupe.
- contourner les restrictions d'utilisation des logiciels mis à ma disposition,
- utiliser ou tenter d'utiliser des droits autres que les miens, masquer ma véritable identité ou usurper celle d'autrui,
- quitter mon poste de travail ou un accès en « libre-service » sans me déconnecter ou en laissant des ressources ou des services accessibles sans surveillance,
- empêcher le fonctionnement des applications de sécurité (protections, surveillance...),
- transmettre des droits étendus à une autre personne sans validation préalable du RSSI,
- transmettre ou réinitialiser le mot de passe d'un compte nominatif pour un tiers qui n'en est pas le détenteur.

* Les analyses de typologie de fichiers visant à assurer le bon fonctionnement des infrastructures et protéger le patrimoine informationnel de l'entreprise ne sont pas concernées (exemple : augmentation significative de la volumétrie d'un répertoire)

** Assistance à distance : Prise en main d'un poste à distance en utilisant la session de l'utilisateur déjà connecté (les utilisateurs, local et distant, partagent le même écran et les informations de l'utilisateur local)

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.