Extrait de la

Politique en matière de Sécurité de l'Information (PSI) de BK Group

De par son engagement quotidien à un comportement éthique et déontologique, BK Group est très attachés au respect de la sécurité de ses informations et de celles de ses clients.
C'est pourquoi BK Group a créé cette politique de sécurité de l'information et demande à tous ses collaborateurs, salaries comme fournisseurs, de la respecter.

Nous nous engageons à :

- Assurer et respecter l'intégrité, la confidentialité et la disponibilité des informations que nous manipulons
- Respecter nos exigences de la sécurité de l'information et celles de nos clients
- Respecter les exigences légales et réglementaires auxquelles nous sommes soumis en matière de sécurité de l'information
- Apprécier et gérer les risques liés à la sécurité de l'information, et les revoir chaque année
- Revoir annuellement cette politique en fonction des orientations stratégiques de BK Consulting et des évolutions des contextes externes et internes
- Contrôler régulièrement la mise en œuvre des mesures de sécurité issues de la Politique et des Objectifs de Sécurité de l'Information
- Améliorer en permanence notre système de gestion de la sécurité de l'information, notamment au travers du « Plan de Traitement de Risques annuel »

Paraphe

Ces engagements se traduisent par les objectifs suivants :

Pour la protection des données, applications et matériels :

- Empêcher la perte, l'endommagement, le vol ou la compromission des données, des applications et des matériels de BK Group et de ceux de ses clients, au travers d'un niveau de protection approprié
- Protéger constamment les données, applications et matériels contre les logiciels malveillants
- Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) des données stockées sur les applications et matériels
- Limiter au strict nécessaire par le biais d'autorisations adaptées l'accès aux données et aux moyens de traitement de l'information associés ; empêcher les accès non-autorisés.
- Garantir l'exploitation et la disponibilité des applications et matériels

Au niveau des accès physiques :

- Empêcher en permanence les accès physiques non autorisés, les intrusions dans les salles et bâtiments qui permettent l'accès aux données et aux matériels

Concernant l'engagement des salariés et sous-traitants en matière de sécurité :

En tant que salariés et sous-traitants :

- Bien comprendre ses responsabilités en matière de sécurité de l'information chez nos clients et en interne ; assumer pleinement ses responsabilités sur ce sujet
- Être sensibilisé à la sécurité de l'information pour les rôles qu'ils assument
- Maintenir ses engagements vis-à-vis de la sécurité de l'information durant toute la vie du contrat de travail ou de sous-traitance et après son terme
- Être responsable de la protection de ses informations d'authentification.

Dans le cadre d'une situation de travail en mobilité :

- Assurer la sécurité de l'information en situation de télétravail
- Assurer la sécurité de l'information dans l'utilisation d'appareils mobiles
- Respecter les règles de sécurité de l'information dans le cadre du télétravail

D'une manière générale :

- Empêcher l'interruption des activités de BK Group
- Continuer à assurer la sécurité des données, des applications et du matériel en situation de continuité de l'activité
- Considérer la sécurité de l'information tout au long du cycle de vie des données d'une part et des applications et matériels d'autre part
- Assurer la protection de l'information sur les réseaux
- Empêcher l'exploitation des vulnérabilités techniques
- Gérer de façon cohérente et efficace les incidents liés à la sécurité de l'information

Paraphe