

Politique de sécurité de l'information

Le système de gestion de la sécurité de l'information des sociétés du groupe Bakioglu Holding repose sur les principes fondamentaux suivants :

Fiabilité (Confidentialité) : Empêcher que des informations ne soient disponibles ou accessibles à des personnes, entités ou autres systèmes d'exploitation non autorisés.

Intégrité : Préserver l'intégrité et l'exactitude des actifs.

Accessibilité : Garantir l'accès et la disponibilité sur demande d'une personne autorisée.

- Établir, développer et assurer la pérennité et l'amélioration continue du système de gestion nécessaire pour identifier, évaluer et mettre en œuvre des contrôles relatifs aux exigences de sécurité, aux risques, aux vulnérabilités et aux opportunités en ce qui concerne notre stratégie commerciale et nos processus de sécurité de l'information.
- Garantir le respect intégral des exigences légales, opérationnelles et contractuelles, et assurer la confidentialité, l'intégrité et la disponibilité de toutes les informations stockées sur supports physiques et électroniques,
- Garantir le respect intégral de toutes les exigences légales en matière de législation douanière,
- Établir des principes de travail pour la gestion des risques, ainsi que développer et mettre en œuvre des mesures de contrôle pour les risques liés à la sécurité. Analyse en permanence des attentes et des évolutions technologiques afin de surveiller les risques,
- Atténuer l'impact des risques liés à la sécurité de l'information sur la continuité des activités et assurer cette continuité,
- Posséder les compétences nécessaires pour réagir rapidement aux incidents potentiels de sécurité de l'information et en atténuer l'impact,
- Minimiser les risques liés à la sécurité de l'information, sensibiliser les utilisateurs et les employés à la sécurité de l'information et s'assurer qu'ils sont bien conscients de leurs responsabilités,
- Évaluer la performance en matière de sécurité de l'information et l'efficacité du système de gestion de la sécurité de l'information par rapport aux objectifs définis,
- Assurer la protection des données personnelles,
- Établir et évaluer les exigences de sécurité de l'infrastructure électronique desservie, l'améliorer en s'adaptant aux évolutions technologiques et assurer la continuité du service,
- S'assurer que les prestataires de services externes respectent les exigences et les nécessités requises par le système de sécurité de l'information,
- Assurer un niveau de sécurité acceptable pour l'accès externe au système,
- Définir les exigences en matière de sécurité de l'information des tiers, des clients et des fournisseurs, et garantir leur conformité au système de gestion de la sécurité de l'information,
- Préserver et renforcer la réputation du groupe en cas d'impacts négatifs liés à la sécurité de l'information,
- Établir les normes de sécurité de l'information pour les sociétés du groupe, les auditer à intervalles réguliers et en garantir la conformité.
- Évaluer les impacts potentiels du changement climatique sur la sécurité de l'information et mettre en œuvre les mesures nécessaires pour atténuer ces impacts.