

POLITIQUE DE SECURITE DE L'INFORMATION

PORTEE DE LA SECURITE DE L'INFORMATIQUE

Cette politique concerne toutes les unités ayant accès à l'infrastructure des technologies de l'information de la société, les utilisateurs ayant accès aux systèmes de l'information en tant que Tierce Partie et les fournisseurs de service, de logiciel et de matériel dans le cadre de soutien technique aux systèmes de l'information.

La sécurité de l'information du Holding Ustunberk ; a pour objectif de permettre la continuité des systèmes d'information, de sensibiliser ses employés et d'accroître leur niveau d'adaptation à leurs besoins de sécurité, de permettre la conformité avec les Tierce Parties et de mettre en œuvre de manière active les contrôles de sécurité technique actuelle afin de protéger la réputation, la fiabilité, les biens de l'information et afin d'avoir une continuité des activités avec le moindre d'interruption possible, notre société est gérée avec une approche de risque

NOS OBJECTIFS DE SECURITE DE L'INFORMATION;

- Documenter notre système de gestion de sécurité de l'information de façon à satisfaire les exigences des normes ISO 27001, permettre son amélioration continue.
- Agir en fonction de la vision et la mission de notre société,
- Diminuer l'impact des risques de sécurité de l'information axée sur la continuité des opérations et permettre une continuité des opérations,
- Protéger et développer la réputation du holding des impacts négatifs provenant de la sécurité de l'information,
- Permettre la confidentialité, l'intégrité et l'accessibilité de toute information gardée sur papier et électroniquement tout en étant conforme aux obligations légales, clientèles et aux conditions opérationnelles et aux conditions de contrat.
- Accroître la sensibilité des utilisateurs et des employés sur la sécurité de l'information et les en rendre conscients afin de minimiser le plus possible les risques de sécurité de l'information,
- Déterminer, évaluer les besoins sécuritaires de l'infrastructure électronique desservie, les développer tout en suivant de près les développements technologiques pour permettre une continuité du service.
- Fournir un niveau de sécurité acceptable afin de permettre un accès au système de l'extérieur de la société,
- Définir les besoins en sécurité de l'information des Tierces Parties, des clients et des fournisseurs et s'assurer qu'ils sont conformes au système de gestion de la sécurité de l'information.
- Protéger la confidentialité des données critiques concernant les objectifs stratégiques, la conception, la fabrication, la vente de nos produits et services, les informations d'approvisionnement, des clients et des employés.
- Gérer de façon intégrée nos activités avec d'autres systèmes de gestion que nous utilisons afin de détecter à temps les situations contraires à la sécurité de l'information et y intervenir tout de suite.