



SUPERVIZOR

Digitized audit and internal control.
No setup. For real.

Déclaration de la Politique Générale de la Sécurité de l'information

L'orientation stratégique en matière de sécurité de l'information n'est que l'image du cadre de gouvernance de Supervizor. Elle constitue le fondement des processus, directives, procédures, pratiques et autres mesures nécessaires pour assurer la protection de l'information et des actifs informationnels.

La direction générale a initié une démarche de sécurisation du système d'information, prenant en compte, dans un esprit pragmatique, les contraintes et les exigences de chacun. La Direction soutient cette démarche et affirme son engagement à renforcer la sécurité de l'information à tous les niveaux afin de :

- **Protéger sa réputation contre les dommages pour la réputation en cas de cyberattaques ou divulgation de données ;**
- **Gagner la confiance des clients et des partenaires ;**
- **Protéger les données de Supervizor contre l'altération ou l'indisponibilité ;**
- **Protéger les secrets industriels de Supervizor contre le vol ;**
- **Protéger les données des clients de Supervizor contre l'accès non autorisé, l'altération ou l'indisponibilité ;**
- **Protéger ses partenaires d'un incident de sécurité de l'information qui aurait pour origine Supervizor.**

Pour atteindre ces objectifs, Supervizor a mis en place son SMSI (Système de Management de la Sécurité de l'Information) conforme à la norme internationale ISO/IEC 27001 et elle a défini sa politique de sécurité du système d'information : le cadre, les principes, les responsabilités et l'organisation mis en place pour répondre à ces enjeux.

Chaque collaborateur est responsable des informations et des ressources qu'il manipule dans le cadre de ses fonctions. Il doit respecter les contraintes liées à la sensibilité de ces informations et ressources.

Chaque responsable de département ou Manager est chargé de contrôler la bonne application de la politique de sécurité du SI dans son périmètre. Il doit notamment s'assurer que ses collaborateurs ont un niveau de connaissance, de compréhension et de compétence suffisant en matière de sécurité afin d'accomplir correctement leurs missions.

Nous comptons ainsi sur l'engagement de tous et l'implication personnelle de chacun de vous pour respecter et mettre en application les principes définis dans la politique de sécurité du système d'information.

La direction Générale