TRIGO est conscient que le traitement des informations est essentiel à la fourniture de ses services et que la sécurité et la protection des informations collectées, traitées et partagées doivent être maintenues. Notre direction s'engage non seulement à garantir le respect des exigences applicables (légales, réglementaires et celles émanant des clients, fournisseurs, collaborateurs et autres parties intéressées), mais également à améliorer en continu le système de management afin d'assurer la disponibilité, l'intégrité et la confidentialité des informations sensibles.

À cette fin, nous nous efforçons de:

- Identifier et gérer les risques et les opportunités en matière de sécurité de l'information.
- Sensibiliser les collaborateurs aux risques et développer une culture de la sécurité de l'information au moyen de formations, de communications et du partage des enseignements tirés des retours d'expérience, afin de permettre à chaque collaborateur de l'organisation de rester informé des meilleures pratiques en matière de sécurité.
  - → TRIGO vise à garantir qu'au moins 90 % de ses collaborateurs auront reçu une formation en cybersécurité d'ici fin 2027.
- Protéger les données à caractère personnel dans le respect de nos obligations légales.
- Déployer et maintenir des infrastructures informatiques et des systèmes numériques stables, sécurisés et hautement disponibles, soutenus par une stratégie globale de cybersécurité, incluant la maîtrise des processus externalisés.
- Détecter, signaler et répondre efficacement aux incidents de sécurité de l'information.
- Déployer et maintenir des infrastructures informatiques et des systèmes numériques stables, sécurisés et hautement disponibles, appuyés par une stratégie globale de cybersécurité, incluant la maîtrise des processus externalisés.
- Surveiller en continu notre environnement informatique à l'aide d'une combinaison d'outils de supervision internes et de plateformes externes d'évaluation de la cybersécurité, permettant une visibilité permanente sur notre exposition aux vulnérabilités et aux menaces.
  - → TRIGO vise à maintenir une note minimale de cybersécurité de 750 sur 1000, mesurée par des plateformes indépendantes d'évaluation de la cybersécurité, reflétant une maîtrise solide de sa surface d'attaque externe et un effort continu pour identifier et corriger les vulnérabilités.
- Réaliser des audits de sécurité réguliers afin de garantir l'efficacité des contrôles mis en place et de favoriser l'amélioration continue.
- Tester et maintenir les Plans de Reprise d'Activité pour nos systèmes informatiques opérationnels.

Cette politique est rédigée par le Responsable de la Sécurité des Systèmes d'Information (CISO), en coordination avec le Responsable de la Protection des Données du Groupe, et approuvée par le CEO et le Directeur Général Adjoint (Deputy CEO). Cette politique est soutenue par plusieurs politiques, processus et ressources afin d'assurer sa mise en œuvre.

Elle s'applique à toutes les entités TRIGO dans le monde, y compris à l'ensemble des collaborateurs, prestataires et tiers ayant accès aux systèmes d'information de TRIGO.

Sa mise en œuvre repose sur un modèle de responsabilité partagée :

- La fonction IT du Groupe est responsable de la définition, du déploiement et du maintien des infrastructures informatiques globales, des mesures de cybersécurité, des activités de surveillance et des capacités de reprise après sinistre.
- Les entités locales et les utilisateurs sont responsables du respect des règles définies, de la protection des actifs informationnels et de leur contribution à la gestion des risques et des incidents liés à la sécurité de l'information.

Ainsi, bien que certains contrôles soient gérés de manière centralisée au niveau du Groupe, le Directeur Général de chaque entité est responsable de la bonne application de cette politique dans son périmètre.

Le Groupe favorise également l'amélioration continue en suivant les indicateurs pertinents et en mettant en œuvre des actions correctives lorsque cela est nécessaire. Cette politique fait l'objet d'une revue annuelle dans le cadre du processus de Revue de Direction. Cette revue prend en compte les enjeux internes et externes, les événements et impacts significatifs liés à la sécurité, ainsi que l'orientation stratégique du Groupe, afin de garantir la pertinence continue, l'efficacité et l'amélioration continue de la politique.

Nous comptons sur l'ensemble de nos collaborateurs pour adopter les comportements appropriés et contribuer à l'amélioration de nos pratiques de sécurité en faisant remonter les idées d'amélioration.

Matthieu RAMBAUD
CEO

Benoît LEBLANC
Deputy CEO

Version #	Date d'applicabilité (mm/dd/yy)	Page(s)	Description des changements
A	07/15/26	Toutes	Contenu initialement inclus dans le document PR.MAN.WW.09.FR-A – Sécurité de l'information (version du 3 avril 2023). Ce nouveau document introduit également des objectifs quantitatifs.