TRIGO ist sich bewusst, dass die Informationsverarbeitung entscheidend ist, um seine Dienstleistungen zu erbringen, und dass die Sicherheit und der Schutz der erfassten, verarbeiteten und weitergegebenen Informationen aufrechterhalten werden müssen. Unsere Geschäftsführung verpflichtet sich nicht nur dazu, die Einhaltung geltender Anforderungen (gesetzlicher, regulatorischer sowie von Kunden, Lieferanten, Mitarbeitenden und anderen interessierten Parteien) sicherzustellen, sondern auch dazu, das Managementsystem fortlaufend zu verbessern, um die Verfügbarkeit, Integrität und Vertraulichkeit sensibler Informationen zu sichern.

Zu diesem Zweck streben wir Folgendes an:

- Informationssicherheitsrisiken und -chancen identifizieren und steuern.
- Mitarbeitende für Risiken sensibilisieren und durch Schulungen, Kommunikation und den Austausch von Lessons Learned eine Kultur der Informationssicherheit entwickeln, um alle Mitarbeitenden unserer Organisation hinsichtlich bewährter Sicherheitspraktiken auf dem aktuellen Stand zu halten.
  → TRIGO verfolgt das Ziel, sicherzustellen, dass mindestens 90 % seiner Mitarbeitenden bis Ende 2027 eine Schulung zur Cybersicherheit erhalten haben.
- Personenbezogene Daten unter Beachtung unserer gesetzlichen Verpflichtung schützen.
- Stabile, sichere und hochverfügbare IT-Infrastrukturen und digitale Systeme bereitstellen und aufrechterhalten, unterstützt durch eine umfassende Cybersicherheitsstrategie, einschließlich der Kontrolle ausgelagerter Prozesse.
- Informationssicherheitsvorfälle erkennen, melden und wirksam darauf reagieren.
- Stabile, sichere und hochverfügbare IT-Infrastrukturen und digitale Systeme bereitstellen und aufrechterhalten, unterstützt durch eine umfassende Cybersicherheitsstrategie, einschließlich der Kontrolle ausgelagerter Prozesse.
- Unsere IT-Umgebung kontinuierlich durch eine Kombination aus internen Überwachungstools und externen Cyber-Rating-Plattformen überwachen, um eine fortlaufende Transparenz über bestehende Schwachstellen, Bedrohungen und Risiken innerhalb der technischen Systemlandschaft sicherzustellen.
  → TRIGO verfolgt das Ziel, eine Mindestbewertung der Cybersicherheit von 750 von 1000 aufrechtzuerhalten, gemessen durch unabhängige Cyber-Rating-Plattformen, was eine solide Kontrolle über seine externe Angriffsfläche und kontinuierliche Bemühungen zur Identifizierung und Behebung von Schwachstellen widerspiegelt.
- Regelmäßige Sicherheitsaudits durchführen, um die Wirksamkeit der implementierten Maßnahmen sicherzustellen und die fortlaufende Verbesserung voranzutreiben.
- IT-Notfallwiederherstellungspläne für unsere operativen IT-Systeme testen und aufrechterhalten.

Diese Richtlinie wird vom Chief Information Security Officer in Abstimmung mit dem Group Data Protection Officer erstellt und vom CEO und Deputy CEO genehmigt. Diese Richtlinie wird durch mehrere Richtlinien, Prozesse und Ressourcen unterstützt, um ihre Umsetzung sicherzustellen.

Sie gilt für alle TRIGO-Niederlassungen weltweit, einschließlich aller Mitarbeitenden, Auftragnehmenden und Dritten, die auf TRIGO-Informationssysteme zugreifen.

Ihre Umsetzung beruht auf einem Modell geteilter Verantwortung:

- Die Gruppen-IT-Funktion ist verantwortlich für die Definition, Bereitstellung und Aufrechterhaltung globaler IT-Infrastrukturen, Cybersicherheitsmaßnahmen, Überwachungsaktivitäten und IT-Notfallwiederherstellungsfähigkeiten.
- Lokale Einheiten und Nutzer sind verantwortlich für die Einhaltung der festgelegten Regeln, den Schutz von Informationswerten und den Beitrag zum Management von Informationssicherheitsrisiken und -vorfällen.

Daher ist, auch wenn einige Maßnahmen zentral auf Gruppenebene gesteuert werden, der Geschäftsführer jeder Niederlassung für die ordnungsgemäße Anwendung dieser Richtlinie innerhalb seines Verantwortungsbereichs rechenschaftspflichtig.

Die Gruppe fördert außerdem die fortlaufende Verbesserung durch die Überwachung relevanter Indikatoren und die Umsetzung von Korrekturmaßnahmen, sofern erforderlich.

Diese Richtlinie unterliegt einer jährlichen Überprüfung im Rahmen des Managementbewertungsprozesses. Diese Überprüfung berücksichtigt interne und externe Themen, wesentliche Sicherheitsereignisse und Auswirkungen sowie die strategische Ausrichtung der Gruppe, um die fortdauernde Relevanz, Wirksamkeit und fortlaufende Verbesserung der Richtlinie sicherzustellen.

Wir verlassen uns darauf, dass alle unsere Mitarbeitenden die richtigen Verhaltensweisen übernehmen und zur Verbesserung unserer Sicherheitspraktiken beitragen, indem sie Verbesserungsideen an die zuständigen Stellen weitergeben.

Matthieu RAMBAUD
CEO

Benoît LEBLANC
Deputy CEO

Version #	Gültigkeitsdatum (mm/dd/yy)	Seite(n)	Beschreibung der Änderung(en)
A	07/15/26	Alle	Inhalt ursprünglich enthalten in Dokument PR.MAN.WW.09.EN-A Information security (Version vom April 3, 2023). Dieses neue Dokument führt außerdem quantitative Zielwerte ein.