TRIGO is aware that information processing is key to deliver its services and that the security and protection of collected, handled and shared information must be maintained. Our management is committed not only to ensuring compliance with applicable requirements (legal, regulatory and from customer, suppliers, employees and other interested parties), but also to continuously improve the management system to secure the availability, integrity and confidentiality of the sensitive information.

To this end, we strive to:

- Identify and manage information security risks and opportunities.
- Make aware employees on risks and develop a culture of information security through trainings, communications and lessons learned sharing to keep every employee of our organization up to speed on best security practices.
  - → TRIGO aims to ensure that at least 90% of its employees have received training on cybersecurity by the end of 2027.
- Protect personal data in respect of our legal duty.
- Deploy and maintain stable, secure, and highly available IT infrastructures and digital systems, supported by a comprehensive cybersecurity strategy, including the control of outsourced processes.
- Detect, report and respond effectively to information security incidents.
- Deploy and maintain stable, secure, and highly available IT infrastructures and digital systems, supported by a comprehensive cybersecurity strategy, including the control of outsourced processes.
- Continuously monitor our IT environment through a combination of internal monitoring tools and external cyber rating platforms providing ongoing visibility on our exposure to vulnerabilities and threats.
  - → TRIGO aims to maintain a minimum cybersecurity rating of 750 out of 1000, as measured by independent cyber rating platforms, reflecting a solid control over its external attack surface and a continuous effort to identify and remediate vulnerabilities.
- Perform regular security audits to ensure the effectiveness of implemented controls and drive continuous improvement.
- Test and maintain Disaster Recovery Plans for our operational IT systems.

This policy is drafted by the Chief Information Security Officer in coordination with the Group Data Protection Officer and approved by the CEO and deputy CEO. This policy is supported by several policies, processes, and resources to ensure its implementation.

It applies to all TRIGO entities worldwide, including all employees, contractors, and third parties accessing TRIGO information systems.

Its implementation relies on a shared responsibility model:

- The Group IT function is responsible for defining, deploying, and maintaining global IT infrastructures, cybersecurity measures, monitoring activities, and disaster recovery capabilities.
- Local entities and users are responsible for complying with the defined rules, protecting information assets, and contributing to the management of information security risks and incidents.

Therefore, while some controls are centrally managed at Group level, the General Manager of each entity is accountable for the proper application of this policy within their scope.

The Group also promotes continuous improvement by monitoring relevant indicators and implementing corrective actions where necessary.

This policy is subject to an annual review as part of the Management Review process. This review takes into account internal and external issues, significant security events and impacts, and the Group's strategic direction, in order to ensure the continued relevance, effectiveness and continuous improvement of the policy.

We rely on all our employees to adopt the right behaviors and to contribute to the improvement of our security practices by escalating ideas for improvement.

Matthieu RAMBAUD
CEO

Benoît LEBLANC
Deputy CEO

Version #	Applicability date (mm/dd/yy)	Page(s)	Description of change(s)
A	07/15/26	All	Content initially included in document PR.MAN.WW.09.EN-A Information security (version of April 3, 2023). This new document also introduces quantitative targets.