Information security policy

17 April 2023

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, opportunities, and potential incidents appropriately.
- 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.
- Protect personal data in respect of our legal duty.
- Deploy and maintain stable, secure, and highly available infrastructures and digital systems which implies also to implement a cybersecurity strategy and to control outsourced processes.
- Continuously monitor our infrastructures and perform regular security audits.
- Test and maintain Disaster Recovery Plans for our operational IT systems.

This policy is supported by several policies, processes, and resources to ensure its implementation and we regularly invest in the development of our infrastructure and digital systems.

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

Matthieu RAMBAUD
CEO

Benoît LEBLANC
Deputy CEO