

We are a company specialized in providing consulting, design, implementation, administration, operation, maintenance and support services for technology infrastructures and platforms, including Cloud, DevOps, SecOps, FinOps, observability and automation services.

Our way of working is based on closeness to people, transparency, excellence and a commitment to quality. For us, safeguarding the information of customers, employees and collaborators is a way of caring for the people who trust us.

This policy establishes the framework of the Information Security Management System (ISMS) of **LESSTHAN3**, in accordance with the **ISO/IEC 27001** standard.

Its purpose is to protect the **confidentiality, integrity** and **availability** of information, managing risks to an acceptable level and ensuring business continuity. In this way, it allows us to pursue and achieve our main objectives securely: helping organizations understand what is happening, why, and what actions they should take, by transforming metrics, logs, traces and cloud consumption data into actionable operational intelligence that enables them to optimize their performance, reduce operational risk and make better infrastructure decisions.

Our ISMS applies to the entire organization, to our employees, collaborators and suppliers, and to all information, in any medium, as well as to the systems, facilities and services that process it. It is founded on the following principles and guidelines:

- # **Risk management:** periodically identify, assess and treat risks, with acceptance criteria approved by Management.
- # **Access control:** least privilege; strong authentication and periodic review of permissions.
- # **Information classification and handling:** all information is classified and handled according to its level of sensitivity.
- # **People security:** confidentiality agreements, ongoing training and awareness, and acceptable use of assets.

- # **Physical and technological security:** protection of facilities and equipment, backups, encryption, vulnerability management and change control.
- # **Suppliers:** require equivalent security levels from third parties that access **LESSTHAN3** information.
- # **Incidents and continuity:** detect, report and resolve incidents quickly, and have tested continuity plans in place.
- # **Compliance:** strict compliance with applicable legislation [for example, GDPR, LOPDGDD, Regulation (EU) 2024/1689 (AI)], with applicable information security requirements, with contractual obligations and with any other commitment undertaken by the organization.
- # **Continuous improvement:** of the Information Security Management System as well as of our processes and the services we provide.

The Management of LESSTHAN3 is committed to promoting this policy, providing the resources necessary for the operation of the ISMS, fostering information security awareness and encouraging its continuous improvement.

In Oviedo, on 2 March 2026

Signed: The Management of **LESSTHAN3**



Code:	Policy	Revision:	00	Format revision date:	02/03/2026	Classification:	PUBLIC documentation
-------	--------	-----------	----	-----------------------	------------	-----------------	----------------------