Information Security Policy

GLO-POL-018

Ovarro is a global company which operates an Information Security Management System (ISMS) certified to ISO 27001.

The certified scope of our ISMS is:

"Assembly, installation, commissioning and service of systems and products for telemetry purposes, SCADA, automation and management information for the energy, water and utility markets."

Intended Outcomes of the ISMS

Through the use of appropriate information processing assets, we will preserve the following attributes of information:

- Confidentiality - ensuring information is accessible only to permitted entities.
- Integrity - safeguarding the accuracy and completeness of information and processing methods.
- Availability - ensuring access to information for permitted entities where and when required.
- Privacy - Processing personal data solely by compliant means whilst protecting the rights of individuals.

Our Commitment

We will ensure that:

- Diligence and due care will be taken when processing any information relevant to our business activities.
- We process only information that is needed, and such information is complete and accurate.
- We only make information available to those who need to see it.
- Any relevant business, regulatory, legislative and information security requirements are understood and met.
- The effectiveness of our ISMS is assessed through a suite of information security objectives that are monitored and measured on a rolling basis.
- The integrity of our ISMS is maintained when changes are planned and implemented.
- We operate in a risk-aware culture and respond effectively to any information security issues.
- We continually improve our ISMS.

Supply Chain Assurances

Ovarro requires the following minimum level of information security conformity from all third-party organisations engaged as suppliers:

- Any actual or suspected compromise of confidentiality, integrity, availability, or privacy must be reported to Ovarro immediately and without undue delay. This includes incidents, near-miss events, and security weaknesses that could affect Ovarro systems, services, or data.
- Suppliers must comply at all times with all applicable legislative, regulatory, statutory, and contractual information security requirements relevant to the products or services they provide to Ovarro.
- Suppliers must adhere to Ovarro's supplier management and information security processes, including participation in audits, providing evidence of controls upon request, and supporting ongoing assurance activities as required.

Approval	Date
	04/02/26
Amer Khayyat, Group CEO	