POL Management System Policy

Version history

Version	Date	Author	Approved by
1	13/07/2026	Manuele Pola	Gabriele Venier

Table of contents

- Purpose
- Scope
- Normative references
- Terms and definitions
- Roles and responsibilities
- Management system commitment and objectives
- Archiving and updating
- Reference documents

Purpose

This policy sets out the strategic direction through which Visup's **Top Management** steers the Information Security Management System (ISMS). Visup designs and develops cloud SaaS platforms that collect, manage and leverage data generated by industrial machines and professional appliances, enriching it with artificial intelligence, e-learning and troubleshooting capabilities. Its mission is to turn this data into value for B2B customers, while its vision is to be a reliable partner, including in terms of cybersecurity, for manufacturers operating in Europe and the United States.

From this mission stems the decision to make information security a driver of growth. The organization recognizes that the confidentiality, integrity and availability of the data entrusted to it by customers are essential conditions for creating value over time, for responding to customers' assessment requests and for improving its own internal organization. The policy therefore provides the framework for setting ISMS objectives and for guiding all the policies and procedures that derive from it.

Scope

The policy applies to Visup's entire ISMS and, in particular, to the design, development, delivery and management of digital solutions, cloud services, web applications and software for the visualization and analysis of complex data, together with IT and strategic consulting services. It covers the SaaS platforms for the HoReCa and industrial sectors, support and maintenance services and custom developments. It applies to the operational site at Via Taboga 307, Gemona (UD), to all personnel, including **Top Management**, and to suppliers and partners that process information belonging to the organization or its customers.

Normative references

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regulation (EU) 2016/679
- Regulation (EU) 2023/2854
- Regulation (EU) 2024/2847

Terms and definitions

- **Policy**: intentions and direction of an organization, as formally expressed by its top management.
- **Top management**: person or group of people who directs and controls an organization at the highest level.
- **Management system**: set of interrelated or interacting elements of an organization to establish policies, objectives and processes to achieve those objectives.
- **Objective**: result to be achieved.

- **Continual improvement**: recurring activity to enhance performance.
- **Interested party**: person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
- **Documented information**: information required to be controlled and maintained by an organization and the medium on which it is contained.
- **Information security**: preservation of the confidentiality, integrity and availability of information.

Roles and responsibilities

- **Top Management**: establishes, approves and keeps the policy up to date, ensures its consistency with the business strategy and provides the resources needed to implement it.
- **Chief Executive Officer / CEO**: integrates information security objectives into the business strategy and promotes a security-oriented corporate culture.
- **Management System Manager**: maintains the policy as documented information, oversees its dissemination and publication and submits it for review together with the ISMS objectives.
- **CTO**: translates the policy commitments into the security architecture of the platforms and the cloud infrastructure.
- **DPO**: ensures that the policy commitments are consistent with personal data protection obligations.
- **Project Manager**: incorporates the policy requirements into projects and into relationships with the customers and suppliers involved.
- **Personnel**: know the policy, apply it in their own activities and report to the **Management System Manager** any situation that could compromise it.

Management system commitment and objectives

Visup adopts this policy as an expression of its mission and keeps it appropriate to the context in which it operates: a small company with a single site, providing cloud services to B2B manufacturers and relying on critical suppliers for infrastructure and artificial intelligence. The *Context analysis* and the risk assessment provide the basis on which **Top Management** establishes and updates this direction.

Top Management commitments

The organization is committed to:

- protecting the confidentiality, integrity and availability of its own and its customers' information processed by the platforms and cloud services;
- meeting the applicable information security requirements, whether legal, regulatory, contractual or arising from interested parties;

- applying a risk-based approach, treating risks in proportion to their impact on the business;
- integrating security by design into software development and infrastructure management;
- ensuring the resources, competence and awareness necessary for the ISMS to function;
- continually improving the suitability, adequacy and effectiveness of the ISMS.

Framework for objectives

The policy provides the framework within which the organization sets its information security objectives. Visup pursues measurable objectives, consistent with these commitments and with the outcome of the risk assessment, and records them in the *MOD Improvement programme*, which for each objective specifies the planned action, the person responsible, the resources allocated, the timeframe and the monitoring indicator. **Top Management** reviews the objectives and their progress at least once a year, as part of the management review described in the *PRO Management review procedure*. Specific guidelines for the protection of information assets are set out in the *POL Information security policy*, while the governance of the ISMS is described in *PRO Management processes*.

Policy availability and communication

Visup is committed to making the policy known to those who must apply it and accessible to those who have an interest in it:

Area	Commitment
Documented information	The **Management System Manager** maintains the policy as documented information and keeps it under control in accordance with the *PRO Documented information management procedure*, following approval by **Top Management**.
Internal communication	The **Management System Manager** communicates the policy to all personnel through the internal communication channels defined in the *PRO Communication management procedure*.
Interested parties	Visup publishes the policy on the company website, where customers, prospective customers and other interested parties can freely consult it.

Archiving and updating

The **Management System Manager** archives the policy in electronic format in the ISMS document system, retaining superseded versions in accordance with the *PRO Documented information management procedure*. **Top Management** reviews the policy at least once a year during the management review, and in any case whenever there are significant changes in the context, the applicable requirements or the risks; the **Management System Manager** is responsible for updating it and **Top Management** approves each new version.

Reference documents

- Context analysis
- MOD Improvement programme
- PRO Management review procedure
- POL Information security policy
- PRO Management processes
- PRO Documented information management procedure
- PRO Communication management procedure