



INFORMATION SECURITY POLICY

At Anyverse, we protect the information we work with throughout all phases of the lifecycle of our simulation and synthetic data generation platform for AI-based perception systems: design, development, deployment, operation, support, and maintenance.

This protection is carried out in coherence with the principles defined in our responsible and sustainable governance policy, which reflects our commitment to ethical business management, the promotion of an inclusive culture, and environmental protection.

Taking these principles as a reference, we adopt the following fundamental commitments for the protection of information:

- **Confidentiality:** Information managed by Anyverse shall be accessible only by duly authorized and identified persons, through established channels and controls.
- **Integrity:** We guarantee that information remains complete, accurate, and free from unauthorized manipulation.
- **Availability:** We ensure that information is accessible and usable by authorized users when required.

These principles constitute the basis for establishing our information security objectives and for the continuous improvement of our management system.

Information Security Objectives

Anyverse establishes the following objectives to guarantee the protection of information and the continuous improvement of its management system:

- Protect the confidentiality of sensitive information, ensuring that **100% of accesses to critical systems** are authenticated and managed under the principle of least privilege.
- Maintain the availability of essential services, achieving an **internal availability SLA of 99.5%** in the systems supporting the synthetic data generation platform.
- Preserve data integrity, ensuring that **100% of relevant changes** in code, configuration, and infrastructure have traceability via version control and review tools.
- Reduce the impact of security incidents, achieving that **90% of detected incidents are analyzed and closed within a maximum period of 5 working days**.
- Guarantee the technical robustness of systems, maintaining at all times **zero (0) pending technical vulnerabilities of High or Critical severity**, and promoting proactive remediation of Medium severity vulnerabilities.



- Increase staff awareness, achieving an **annual participation rate of 100%** in mandatory training on security and best practices.
- Ensure regulatory and contractual compliance, performing at least **one annual review** of compliance with legal, regulatory, and automotive sector (and related) client requirements.
- Adequately manage risks and continuous improvement, ensuring that **100% of corrective actions** derived from internal or external audits are executed within the committed timeframe.

Anyverse Management assumes the commitment to comply with and enforce all applicable legal, regulatory, and contractual requirements, promoting compliance with this policy among all personnel, and applying, when necessary, disciplinary measures aimed at strengthening the security culture and ensuring the effectiveness of the management system.

This policy will be reviewed periodically to ensure its validity and effectiveness. Any relevant changes will be communicated to employees and stakeholders, ensuring their correct application.

In Madrid, on October 15, 2025

Victor González

CEO