# Information Systems Security Policy

FR-01-POL-0005

**The CIS Group Information Systems Security Policy contributes to:**

- Ensure the continuity of the CIS Group's activities.
- Prevent leakage of sensitive information.
- Build the confidence of Group employees in the use of the resources made available to them.

**This policy defines the security measures applicable to the Information Systems of the CIS Group. It is based on 10 strategic principles:**

1. When mastery of its Information Systems requires it, the CIS Group calls on trusted operators and service providers.

2. Any Information System of the CIS Group must be subject to a risk analysis allowing a preventive consideration of its security, adapted to the challenges of the system considered. This analysis is part of a process of continuous improvement of system security, throughout its lifetime. This approach should also make it possible to keep up to date an accurate mapping of the information systems in service.

3. The human and financial resources devoted to the security of Information Systems of the CIS Group must be planned, quantified and identified within the global resources of Information Systems.

4. Strong authentication methods for CIS Group employees on Information Systems must be put in place.

5. The CIS Group's Information Systems management and administration operations must be traced and controlled.

6. The protection of Information Systems must be ensured by the rigorous application of precise rules. These rules are the subject of the guidelines for the security of Information Systems.

7. Each employee of the CIS Group, as a user of an Information System, must be informed of their rights and duties but also trained and made aware of cybersecurity. The technical measures implemented by the CIS Group in this area must be known to all.

8. Administrators of Information Systems must apply, after training, the basic rules of cyber hygiene.

9. The products and services acquired by the various departments and intended to ensure the security of the CIS Group Information Systems must be subject to an assessment and prior validation of their level of security by the person responsible for the Information System Security of the CIS Group.

10. Information considered sensitive, due to its confidentiality, integrity or availability needs, is hosted on the Information System of the CIS Group.

Régis Arnoux, Chairman & CEO