PURFLUX POLICY

PURFLUX GROUP

POLI-GRP-1009

GROUP INFORMATION SECURITY POLICY

Revision	Author	Job Title	Last Update	Due Date
01	Julien GRANGE	Group CEO	28/03/2026	31/12/2026

1. PURPOSE

PURFLUX GROUP considers that protecting its information assets is an essential responsibility towards its employees, customers, and all stakeholders. In an increasingly complex digital environment, the Group is therefore fully committed to preserving the confidentiality, integrity, and availability of its information, and to managing information security risks in a structured and proactive manner.

This Policy sets out the core principles to be observed by all employees and across all Group sites worldwide, confirming PURFLUX GROUP's commitment to information security as a strategic business enabler and a prerequisite for maintaining the trust of its customers and partners.

2. SCOPE

PURFLUX GROUP ensures systematic control and continuous improvement of information security through an Information Security Management System (ISMS) aligned with the TISAX requirements defined by the ENX Association. This ISMS establishes a structured approach to identifying and managing information security risks across the organization, supporting the confidentiality, integrity, and availability of information assets while meeting customer and partner expectations within the automotive industry. It applies to all PURFLUX GROUP entities involved in design, development, manufacturing, and distribution, including the headquarters and R&D centers, global production sites.

The ISMS covers all personnel and authorized third parties operating within this defined scope, and its effectiveness is maintained through audits, incident monitoring, management reviews, and a continual improvement process.

External logistics providers and manufacturing partners not under PURFLUX GROUP’s operational control remain outside the current scope.

3. PURFLUX GROUP ‘S COMMITMENT

PURFLUX GROUP is committed to protecting the confidentiality, integrity and availability of its information assets. Top management supports and continually improves the Information Security Management System (ISMS) by providing the necessary resources and regularly reviewing its performance.

Information security is a shared responsibility. All employees must protect information, use company resources responsibly, and prevent unauthorized access, loss or misuse.

Compliance with the Information Security Policy is essential to ensure business continuity, safeguard operations, and support the Group's longterm strategic objectives. In addition, the Group is committed to meeting applicable legal, regulatory and customer requirements related to information security to maintain trust and ensure alignment with client expectations.

4. KEY PRINCIPLES

In order to protect the information assets of the Group and its customers, PURFLUX GROUP commits to upholding the following principles:

- **Operate in full compliance with applicable national and international laws,** voluntary requirements, and any policy or procedure in place within the industry that constitutes international best practice in information security, including TISAX / VDA ISA requirements for the automotive sector.
- **Implement, maintain, and continuously improve an Information Security Management System (ISMS)** aligned with the guidelines of ISO/IEC 27001, applicable regulatory requirements, and any other relevant local legislation and standards, ensuring adequate security conditions across all Group operations.
- **Define and share responsibilities at different levels.** Management committees shall translate these guidelines into operational procedures and identify objectives and deployment plans. Every employee must be aware of their individual responsibility in information security and shall therefore follow all required practices.
- **Control access to information systems and data** based on the principle of least privilege. Access rights shall be granted only to the extent necessary for assigned duties, and shall be reviewed and revoked in a timely and controlled manner.
- **Classify information assets** and apply protection measures commensurate with their level of sensitivity. Each asset shall have a designated owner accountable for its protection throughout its lifecycle.

- **Protect the continuity of business operations** by maintaining and regularly testing recovery plans for critical information systems and services, ensuring the Group's ability to respond to and recover from any disruptive event.
- **Raise awareness and provide training** to all personnel on information security requirements, risks, and good practices, in order to stimulate and involve them in maintaining the highest standards of information protection across all sites.
- **Manage security incidents through a formal process.** Any employee who becomes aware of a real or suspected security incident shall report it immediately through the appropriate internal channel, ensuring a swift and effective response.
- **Minimize the risk of unauthorized disclosure of sensitive information** – in particular customer data, technical know-how, and intellectual property – by implementing appropriate technical and organizational controls in all business activities and processes.
- **Promote information security across the entire value chain,** engaging with suppliers, contractors, and business partners to ensure they comply with the principles set out in this Policy and with all applicable local laws in the countries where they operate.
- **Ensure continuous improvement** of information security practices by investing in processes, technologies, and skills that integrate appropriate security standards, evaluating all potential risks, and taking every suitable measure to eliminate or reduce identified vulnerabilities.

Guyancourt, 28th March, 2026

Julien GRANGE

CEO PURFLUX GROUP