INFORMATION SECURITY POLICY

Approved by the Disclosure Committee on September 9th, 2026.

Note: This policy is released in English. In case of divergence between the English version and other translated versions, the English version will prevail.

Document Control

Document Name	Information Security Policy_External_Global
Document Reference Number	APL-IS-POL- 1.1
Classification	Public
Initial Release Date	
Owner	Gyanendra Kumar -Group CISO

Revision History

Version	Description	Reviewed By	Review Date	Approved By	Approve Date
V 1.0	Initial Release				

Distribution

- Documentation Management System
- Intranet (Aperam Flow)
- Public through Aperam Website

Documentation status

This is a controlled document. This document may be printed; however, any printed copies of the document should be controlled. The electronic version is maintained in the file server and that is the controlled copy.

1. Introduction

Aperam is a global player in stainless, electrical and specialty steel and recycling, headquartered in Luxembourg. Information is a critical business asset, and its protection is fundamental to maintaining the trust of customers, partners, and regulators, ensuring business continuity, and meeting all legal and regulatory obligations.

2. Policy Statement

Aperam is committed to safeguarding the confidentiality, integrity, and availability of all information assets under its stewardship. To fulfil this commitment, Aperam has established and continually improves an Information Security Management System (ISMS) aligned with international standards and geographic regulations i.e.ISO/IEC 27001:2022.

Aperam is dedicated to:

- Protecting information from unauthorised access, disclosure, alteration, and destruction.
- Complying with all applicable legal, regulatory, and contractual requirements, including personal data protection requirements (GDPR and LGPD).
- Conducting annual risk assessments and applying security controls across the organisation and supply chain.
- Ensuring prompt detection, reporting, investigation, and resolution of information security incidents.
- Delivering regular security awareness training to all personnel and committing appropriate resources annually.

3. Scope

This policy applies to all Aperam information assets, digital and physical, regardless of location or format. It covers all employees, contractors, temporary staff, and authorised third parties; all information systems, networks, applications, and cloud services; and all supply chain partners, vendors, and sub-processors acting on Aperam's behalf.

4. Security Control Areas

Aperam's Information Security control environment is aligned with **ISO/IEC 27001:2022 Annex A** and **NIST Cybersecurity Framework (CSF)**. A baseline set of mandatory controls establishes a minimum protection level across the Group, supplemented by risk-based measures where the business context requires. Controls are organised across four domains:

Organizational Controls

Information security roles, responsibilities and accountabilities are defined across the organisation, with appropriate segregation of duties and governed supplier and third-party relationships. Relevant controls are assured in line with the requirements of ISO/IEC 27001:2022, are reviewed periodically, and any exceptions are formally recorded. An Information Security Council provides ISMS oversight, supported by ongoing awareness and role-specific training.

People Controls

Security obligations are embedded within employment terms and confidentiality agreements. Regular security awareness training is delivered to all personnel, with refresher and role-specific training provided where appropriate. Relevant controls are assured in line with the requirements of ISO/IEC 27001:2022, and are reviewed periodically.

- ### Physical Controls

  Appropriate physical and environmental protection is maintained across all facilities. Relevant controls are assured in line with the requirements of ISO/IEC 27001:2022, and any exceptions are formally recorded.

- ### Technological Controls

  Appropriate technical safeguards protect the confidentiality, integrity and availability of information across systems, networks and services. Relevant controls are assured in line with the requirements of ISO/IEC 27001:2022, are reviewed periodically, and any exceptions are formally recorded. Personnel receive training to support the secure use of technology.

5. Data Security & Data Protection

Aperam complies with applicable legal, regulatory and contractual personal data protection requirements, including the General Data Protection Regulation (GDPR) and LGPD. Privacy and data protection are embedded by design and by default, with data minimisation, limited retention and restricted access applied to personal data. Aperam Privacy Policy is available on our website: www.aperam.com and the Data Protection Officer can be contacted through dataprotection@aperam.com. Personnel receive periodic data protection and privacy awareness training to support these obligations.

6. Governance & Compliance

Aperam maintains its information security controls in line with the requirements of ISO/IEC 27001:2022 and the NIST Cybersecurity Framework, and reviews them periodically, including across its supply chain and vendor ecosystem. Independent third-party external experts are engaged for the proactive assessment of applicable controls and to benchmark security maturity. Any exceptions to controls are formally recorded, assessed and managed through the Organization policies. Compliance with this policy is mandatory for all personnel and applicable third parties, and is reinforced through ongoing awareness training. Non-compliance may result in disciplinary action and legal consequences wherever applicable.

7. Reporting

All personnel, contractors and third parties are responsible for promptly reporting actual or suspected information security incidents, weaknesses, data breaches or concerns. Reports should be made without delay to the Information Security team at information.security@aperam.com, and personnel are encouraged to report even when unsure, so that potential issues can be assessed early. Awareness training reinforces how and when to report.

Aperam also welcomes the responsible disclosure of potential vulnerabilities by external parties and the security research community. Suspected vulnerabilities should be reported to information.security@aperam.com so they can be investigated and addressed. All reports are treated confidentially and used to strengthen Aperam's security posture.

8. Incident Management & Policy Review

All actual or suspected information security incidents must be reported immediately to the Information Security team. Aperam operates a structured response process covering detection, containment, recovery, and post-incident review. Lessons learned are used to drive continuous improvement. This policy is reviewed at least annually or following significant changes to the threat landscape, business environment, or applicable legal requirements.

9. Management Endorsement

This policy statement is approved by the Disclosure Committee, following approval of the CTIO. It communicates Aperam's commitment to information security to all stakeholders i.e. customers, partners, regulators, and employees; and is available publicly at aperam.com. Further enquiries can be sent to: information.security@aperam.com