



Information Security Policy

INFORMATION SECURITY POLICY

Rev. 0

Issue date: 18 September 2026

Code DSGI02

Information Security Policy

1	PURPOSE AND MANAGEMENT COMMITMENT	pag. 4
2	CONTEXT AND SCOPE	pag. 4
3	PRINCIPLES AND OBJECTIVES	pag. 4
4	GOVERNANCE AND RESPONSIBILITIES	pag. 5
5	INFORMATION SECURITY COMMITMENTS	pag. 5
5.1	Risk and Asset Management	pag. 5
5.2	People and Security Culture	pag. 6
5.3	Access Control and Identity	pag. 6
5.4	Physical, Environmental and Operational Security	pag. 6
5.5	Cryptography and Communications Security	pag. 6
5.6	Acquisition, Development, Maintenance and Vulnerability Management	pag. 7
5.7	Suppliers and Supply Chain	pag. 7
5.8	Incidents, Continuity and Crisis Management	pag. 7
5.9	Personal Data Protection	pag. 7
6	INCIDENT MANAGEMENT AND NOTIFICATION	pag. 8
7	COMPLIANCE, VERIFICATION AND IMPROVEMENT	pag. 8

1. PURPOSE AND MANAGEMENT COMMITMENT

RAFFMETAL S.p.A. considers information security an essential requirement for the continuity of industrial processes, reliability towards customers and partners, protection of information assets and achievement of business objectives.

Management establishes, maintains and continually improves a risk-based Information Security Management System (ISMS) and undertakes to:

- ensure the confidentiality, integrity, availability and authenticity of information;
- meet applicable legal, regulatory, contractual and sector-specific requirements (automotive);
- approve security directions and measurable objectives, making adequate resources, competences and responsibilities available;
- prevent and reduce the impact of incidents on operations, customers, partners and people;
- regularly assess the effectiveness, adequacy and proportionality of the measures adopted and promote the continual improvement of the ISMS.

2. CONTEXT AND SCOPE

RAFFMETAL S.p.A. operates in the production of recycled aluminium alloys and serves, among others, the automotive sector. Security management therefore takes into account the industrial and multi-site nature of the organisation, the interconnection between information technology and operational technology, production continuity, information exchanges across the supply chain and the expectations of customers and other interested parties.

This Policy applies to all persons working for or on behalf of RAFFMETAL S.p.A. and to the processes, information, assets and sites included within the formally approved scope of the ISMS.

3. PRINCIPLES AND OBJECTIVES

The ISMS pursues the following principles and provides the framework for defining and reviewing information security objectives:

1. **Risk-based approach:** promptly identify, analyse, assess and treat risks, assigning priorities and responsibilities.

2. **Proportionate security measures:** adopt technical, operational and organisational measures appropriate to the risk, process criticality and implementation costs.
3. **Information Security by Default:** integrate security requirements into the design, acquisition, development, modification and maintenance of processes, plants, products and systems.
4. **Least privilege and need-to-know principle:** limit access to what is necessary for the role, activity and period, with traceable authorisations subject to periodic review.
5. **Resilience:** prepare the response to incidents and crises.
6. **Shared responsibility:** require personnel and third parties to adopt consistent conduct, timely reporting and compliance with applicable rules.
7. **Continual improvement:** measure effectiveness and efficiency, implement corrective actions and adapt the ISMS to evolving threats, technologies and requirements.

4. GOVERNANCE AND RESPONSIBILITIES

Top Management:

- approves this Policy, the objectives and the methods for implementing risk management measures;
- oversees their implementation; ensures adequate resources; receives periodic information on the status of the ISMS and timely information on significant incidents. The administrative and management bodies exercise the responsibilities required by applicable requirements and participate in appropriate cybersecurity training.

The Security Committee coordinates the implementation of the Policy, risk management, the improvement programme, monitoring and reporting to Management.

Process, asset and risk owners classify and protect the information and assets entrusted to them, cooperate in risk assessment and ensure the implementation of the agreed actions. All personnel and involved third parties must know and comply with the rules, protect credentials and information, and report without delay any events, vulnerabilities, anomalies, losses or suspected incidents through the defined channels.

5. INFORMATION SECURITY COMMITMENTS

5.1 Risk and Asset Management

- Maintain up-to-date inventories of relevant information, applications, infrastructure, devices and IT and OT components, with assigned owners and defined criticality levels.
- Classify and label information and establish consistent rules for creation, access, use, transfer, retention, return and secure destruction.
- Review risks periodically and whenever significant changes, incidents, new threats, regulatory, organisational, technological or site-related changes occur.

5.2 People and Security Culture

- Verify, within the limits of the law, identity and suitability for sensitive roles and define confidentiality and security obligations before, during and after the employment relationship or assignment.
- Provide initial, periodic and role-based training and awareness activities.
- Document participation and verify the effectiveness of training.

5.3 Access Control and Identity

- Manage the full lifecycle of identities and access rights, including approval, least privilege, segregation of duties, periodic reviews and timely revocation.
- Apply strong authentication and, where appropriate or required by the risk, multi-factor authentication; protect privileged, remote and industrial-system access.
- Record and monitor relevant activities in compliance with the law and protect logs against alteration and unauthorised access.

5.4 Physical, Environmental and Operational Security

- Protect sites, areas, plants, technical rooms, media and equipment through perimeters, authorisations, access controls and proportionate environmental measures.
- Define secure configurations, change management, protection against malicious software, updates, monitoring, capacity management and maintenance for IT and OT systems.
- Segregate networks and environments according to risk.

5.5 Cryptography and Communications Security

- Define criteria for the use of cryptography and encryption, key management and protection of data in transit and at rest, according to classification, risk and contractual requirements.

- Use authorised and protected channels for the exchange of information with customers, suppliers and partners, applying non-disclosure agreements where required.

5.6 Acquisition, Development, Maintenance and Vulnerability Management

- Integrate security requirements into specifications, supplier selection, development, testing, acceptance and changes to systems and services.
- Identify, assess, prioritise and remediate vulnerabilities within timeframes consistent with risk; govern exceptions and implement compensating measures.
- Apply formalised change management procedures, including impact assessment, authorisation, testing, post-implementation verification and rollback capability.

5.7 Suppliers and Supply Chain

- Assess the risk of suppliers and external services before engagement and during the relationship, considering criticality, vulnerabilities and dependencies.
- Include proportionate requirements in contracts concerning the relevant information security aspects.
- Monitor the performance and compliance of critical suppliers and promptly manage deviations and significant changes.

5.8 Incidents, Continuity and Crisis Management

- Maintain processes to detect, report, classify, contain, analyse, resolve and document events and incidents, preserving evidence and learning from root causes.
- Define roles, escalation, on-call availability and internal and external communications, coordinating information security, business continuity, crisis management, regulatory and contractual obligations.
- Prepare and test backups and business continuity plans.

5.9 Personal Data Protection

- Integrate applicable personal data protection requirements into the ISMS, coordinating security risk management with the principles of lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy and storage limitation.

- Adopt technical and organisational measures appropriate to the risk to the rights and freedoms of individuals and apply data protection by design and by default to new processing activities and significant changes.
- Coordinate the management of personal data breaches with incident response, ensuring assessment, escalation, documentation and notifications or communications within the applicable time limits.

6. INCIDENT MANAGEMENT AND NOTIFICATION

RAFFMETAL S.p.A. maintains an incident management process that enables reports and notifications to be made without undue delay to the competent authorities, customers and other interested parties, in compliance with the criteria, time limits and methods required by applicable requirements. The process ensures timely escalation, assessment of significance, updates on incident status and a final report on causes, impacts and measures adopted.

The qualification of the incident and communications to service recipients, authorities, customers and other interested parties are coordinated by authorised functions and take into account operational, economic, legal, contractual and reputational impacts, as well as impacts on the rights of individuals. No employee or supplier may independently communicate information on incidents externally unless authorised or required by law.

7. COMPLIANCE, VERIFICATION AND IMPROVEMENT

RAFFMETAL S.p.A. maintains a register of applicable requirements arising from business strategy, laws and regulations, agreements with customers and partners, and the relevant TISAX criteria. Compliance with policies and procedures is verified according to a defined programme through first-line controls, indicators, technical checks, internal audits and independent reviews, with evidence and results retained.

Non-conformities, audit outcomes, incidents, test results and changes in risk generate, where necessary, corrective actions with an assigned owner, priority and deadline. The effectiveness of actions is verified and reported to Management. Security objectives are measurable where practicable and include at least the reduction of risks above the accepted threshold, timeliness of remediation, training completion, continuity test results and incident management.

General Manager

Roberta Niboli

A handwritten signature in black ink, appearing to read 'Roberta Niboli', with a stylized, cursive script.

Per ulteriori informazioni, scrivi a:
info@raffmetal.it

