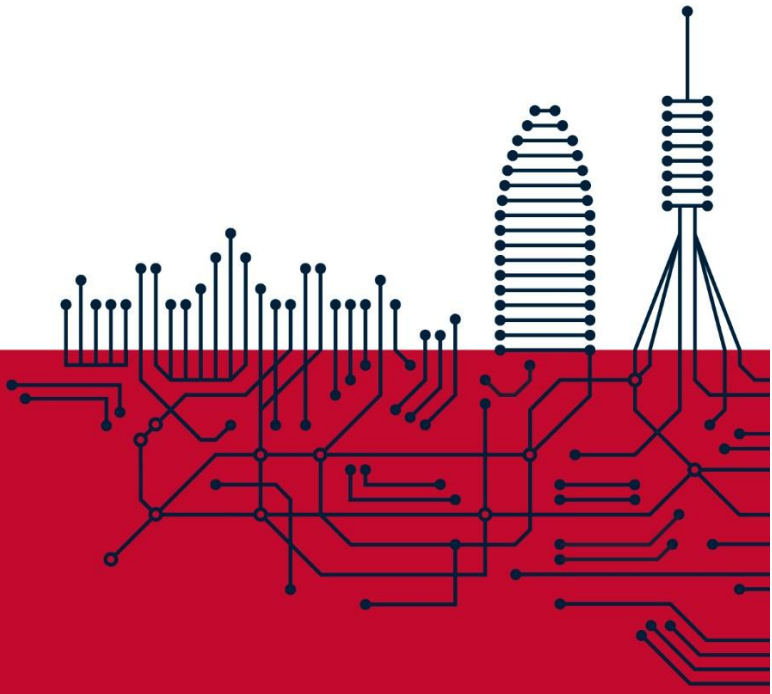
Smarting
ENGINEERING



Information Security Policy

SGSI.PR.01.en v1.2

31/03/2026

1. Management Statement

At **Smarting**, the confidentiality, integrity and availability of the information we process —our own, that of our clients and that of our users— are strategic elements to ensure trust, regulatory compliance and business sustainability.

The Management of **Smarting Engineering, S.L.** declares its commitment to the establishment, implementation, maintenance and continual improvement of the **Information Security Management System (ISMS)**, aligned with ISO/IEC 27001:2022, the Spanish National Security Framework (ENS, RD 311/2022) at MEDIUM category, and complemented by the Business Continuity Management System (BCMS) based on ISO 22301:2019.

Management assumes the following commitments:

1.1. Appropriate to the purpose of the organisation

- **Smarting** develops digital solutions and provides operational support to clients and suppliers, with the Motorcloud platform and its associated services being the essential assets of the organisation.
- Protect the **confidentiality, integrity, availability, traceability and authenticity** of the information handled in the **development of solutions**, the delivery of services and the **support to institutional clients**.
- Integrate information security into all business processes, from design and development through to operations and support.
- Maintain the trust of our clients, in particular of the **transport authorities and operators** who rely on our services.

1.2. Framework for information security objectives

This policy provides the framework for establishing **measurable objectives** for information security, aligned with the strategic direction of the organisation. Objectives are set annually in the Management Review and meet the SMART criteria.

- **RTO** (Recovery Time Objective): target recovery times for critical services.
- **RPO** (Recovery Point Objective): maximum acceptable data loss.
- Operational maturity: **MTTD, MTTR, 3-2-1 backup coverage**, consolidation of SIEM and EDR.
- Regulatory certification: maintenance of ENS MEDIUM and ISO 27001, ISO 22301 certification and preparation for ENS High category.

1.3. Commitment to fulfil applicable requirements

Comply with all **legal, regulatory, contractual and normative requirements** applicable to information security, including:

- **ISO/IEC 27001:2022** and Annex A controls.
- **ENS (RD 311/2022)** at MEDIUM category, with orientation towards High category.
- **RGPD / LOPDGDD** regarding personal data protection.
- **ISO 22301:2019** as a reference for business continuity.
- **NIS2 Directive** as a reference for the organisation’s preparation for future obligations.

- **Contractual requirements** with clients, especially with the Autoritat del Transport Metropolità de Barcelona (ATM).

Provide the **necessary resources** (human, technical, training and financial) for the establishment, implementation and continual improvement of the ISMS.

1.4. Commitment to continual improvement of the ISMS

Promote the **continual improvement** of the ISMS through:

- **Risk analysis and management** periodically using MAGERIT methodology.
- **Internal and external audits** annually (ENS, ISO 27001) and security testing (pentesting).
- **Management reviews** annually in accordance with clause 9.3 of the standard.
- **Management of nonconformities and corrective actions** tracked in YouTrack.
- **Integration of lessons learned** from incidents and exercises.

Promote a **security culture** through periodic training and awareness of all personnel, ensuring the adaptability of the ISMS to technological, organisational, regulatory and threat-environment changes.

2. Scope

This policy applies to all **processes, resources, technologies, infrastructures and people** included in the scope of the ISMS, as well as to suppliers and third parties that may impact the information security of Smarting. This includes:

- The **development of digital solutions** of Smarting, including the Motorcloud platform and its services.
- The **operation of the services** provided to clients and suppliers.
- The associated **technological infrastructure** (data centres, networks, systems and platforms).
- All **personnel** at Smarting, regardless of their contractual arrangement or location.
- The **critical suppliers and third parties** that handle information of Smarting or its clients.

3. Organisational Framework for Security

Smarting has identified and defined the security roles and functions necessary to ensure the protection of information, in accordance with chapter II of **Royal Decree 311/2022** and clause 5.3 of ISO 27001:2022.

3.1. Security Committee

Smarting has established a **Security Committee** that oversees the compliance of the ISMS and the BCMS. Its functions are:

- Coordinate all activities related to information security and business continuity.
- Propose and review the Security Policy and the Business Continuity Policy.
- Approve security standards, procedures and training requirements.
- Oversee the management of incidents, nonconformities and corrective actions.
- Evaluate the activation of continuity plans in the face of disruptions.

3.2. Main roles

The appointments of **CISO**, **Service Owner (RE)** and **DPO** are approved by Management upon proposal by the Security Committee and are reviewed every two years or when the position becomes vacant. The role of Information Owner (**CIO**) is held by the **CTO**.

3.3. Conflict resolution

Smarting has defined the process and hierarchy for the **resolution of authority conflicts** among critical profiles with security responsibilities, applicable to all profiles of the ISMS and BCMS.

4. Risk Analysis and Management

All systems subject to this policy are evaluated through a **risk analysis** based on the **MAGERIT** methodology, assessing threats, vulnerabilities and impacts. This analysis is repeated:

- Regularly, at least once a year.
- When the information handled changes.
- When the services provided change.
- When a serious security incident occurs.
- When serious vulnerabilities are reported.

5. Categorisation of Systems

Smarting classifies its systems in accordance with Annex II of the ENS into **Basic, Medium or High** categories, based on the highest level of the security dimensions evaluated (confidentiality, integrity, availability, traceability and authenticity).

The categorisation process considers the identification of critical systems and assets, the evaluation of the value of information (including special categories under the GDPR), risk analysis, regulatory compliance, dependence between systems, the requirements of the security dimensions and the recovery capacity. When a client determines its own categorisation, **the category established by the client shall prevail**.

6. Personnel Management and Professionalism

All members of **Smarting** have the **obligation to know and comply with** this policy and the Security Standards. The Security Committee is responsible for applying the measures necessary to ensure that the information reaches those affected.

All employees receive **awareness sessions** on security at least once a year, complemented by an ongoing awareness programme and specific training for new joiners.

Personnel dedicated to security tasks have the **appropriate qualification** and receive the specific training necessary to ensure the security of information technologies at all phases of the lifecycle.

The same requirements apply to suppliers providing security-related services, through a formal supplier evaluation procedure.

7. Authorisation and Access Control

The information systems of **Smarting** have formal mechanisms for **authorisation, authentication and traceability** that allow access to be granted, denied or revoked when necessary. Access is limited to what is strictly necessary for the performance of the functions of each person or system.

8. Protection of Facilities

The facilities of **Smarting** are protected against damage that may affect the systems they house and against access by unauthorised persons, in accordance with the current procedures for the protection of facilities and infrastructures.

9. Acquisition of Security Products and Services

Any new acquisition of a **security product or service** that may affect the ISMS is evaluated beforehand from the functional and security requirements perspective. The validation includes formal product testing and verification of compliance.

Security products are prioritised according to the **CPSTIC Catalogue (CCN-STIC 105)**. Where no suitable CPSTIC alternative exists, a formal procedure of justification, validation and approval by the Security Committee is applied.

Every contracted service is evaluated before being put into production to ensure compliance with the minimum security requirements defined in this policy and the Security Standards.

10. Principle of Least Privilege

The ISMS of **Smarting** applies the **Principle of Least Privilege**: each user, process, application or device is granted only the permissions strictly necessary to perform its legitimate functions.

This principle reduces exposure to cyberattacks and prevents the undue accumulation of privileges, applying both to human users and to applications, systems or connected devices that require privileges to perform necessary tasks.

11. System Integrity and Updating

Any **physical or logical change** to the information systems is carried out only after formal approval and following a documented procedure.

Updates, patches and changes in specifications are analysed to prevent the degradation of security and the risks introduced by the changes are managed.

12. Protection of Information Stored and in Transit

Information must be protected throughout its **lifecycle**, both in storage and in transmission, on electronic and physical media. Specific procedures are applied for the handling, labelling, processing and secure disposal of information.

13. Prevention Regarding Interconnected Systems

Connections with external information systems are made with measures of **perimeter protection, access control and activity logging** to detect anomalies. Connections follow the guidelines of the **CCN-STIC** guides published for this purpose.

14. Activity Logging and Malicious Code Detection

Smarting supervises its information systems through **SIEM and EDR tools**, recording relevant events as security incidents. The supervision respects the legal requirements of privacy and is used to verify the effectiveness of controls and compliance with the access control policy.

All corporate equipment is provided with **next-generation antivirus (EDR) tools** with centralised management for the protection, detection, recovery and removal of malicious code.

Incident management is tracked in **YouTrack** in accordance with the **CCN-STIC 817** taxonomy, with notification to the competent authorities (CCN-CERT, AEPD, INCIBE) where applicable.

15. Security Incident Management

The Management of **Smarting** has established a **formal notification procedure** for security incidents. All personnel must notify incidents through the enabled channel (**security@smarting.es**) immediately. This ensures a quick and effective response to incidents and weaknesses.

16. Business Continuity

Smarting has a **Business Continuity Management System (BCMS)** based on **ISO 22301:2019** that complements the ISMS. The BCMS ensures the capacity of the organisation to maintain essential services and recover from disruptions through:

- A **Business Impact Analysis (BIA)** that identifies critical processes and recovery times.
- A **Business Continuity Plan (BCP)** that coordinates the operational response.
- **Disaster Recovery Plans (DRP)** that cover the restoration of infrastructure.
- **Periodic tests and exercises** that validate the effectiveness of the plans.

Continuity management is governed by its specific policy, defined in the **Business Continuity Policy** (SGCN.PR.01.en), which complements this section.

17. Continual Improvement of the ISMS

Management is committed to **developing, implementing, maintaining and continually improving** this Policy and its Management System, particularly valuing the confidentiality, integrity, availability, traceability and authenticity of critical information.

Continual improvement is articulated through **audits, management reviews, indicator analysis, nonconformity management** and the integration of lessons learned from incidents and exercises.

18. Personal Data

Smarting processes personal data in compliance with the **RGPD** and the **LOPDGDD**. Taking into account the state of the art, costs, nature and risks of processing, **Smarting** has applied appropriate technical and organisational measures, including:

- Pseudonymisation and encryption of personal data.
- Ability to ensure the permanent confidentiality, integrity, availability and resilience of processing systems.
- Ability to restore the availability and access to personal data quickly in the event of a physical or technical incident.
- Regular verification, evaluation and assessment processes of the effectiveness of the measures.

The supervision of personal data processing falls upon the **DPO**, appointed in accordance with the GDPR.

19. Structuring of Security Documentation

Security documentation follows the guidelines established in the document control procedures, with measures to structure, manage and control access to the documentation, ensuring its integrity and confidentiality.

The documentation is managed in the **corporate Knowledge Base**, with version control, change traceability and access restricted to authorised personnel: members of the Security Committee, client representatives and authorised consultants or auditors.

20. Documentation and Communication

This policy complies with the communication requirements established in ISO 27001 (5.2):

Requirement	How it is fulfilled
a) Documented information	Version-controlled policy with change log. Signed copy in the security archive.
b) Communicated within the organisation	Training and awareness sessions. Teams channel ENS-ISO. Knowledge base accessible to all personnel.
c) Available to stakeholders	Published on the Smarting corporate website in three languages (ES, CA, EN). Available on request for clients and auditors.

21. Review and Update

This policy is reviewed **annually** as part of the Management Review. It is reviewed **in advance** whenever:

- Significant changes occur in services, infrastructure or organisational structure.
- New legal, regulatory or contractual requirements arise.

- Lessons learned from incidents or exercises require adjustments to the commitments.
- Significant changes occur in the threat environment or in the business context.

Reviews are documented in the Security Committee minutes and in the Management Review.

22. Approval

By approving this policy, the Management of **Smarting Engineering, S.L.** declares its determination and commitment to achieving a level of security appropriate to the needs of the business, ensuring the protection of information, services and people in an integrated manner consistent with the BCMS.

Approved by:	Management of **Smarting Engineering, S.L.**
Date:	31/03/2026
Signature:	The Management

Note: The documents referenced in this policy are periodically updated and are available for consultation by stakeholders. They may be requested at **security@smarting.es**