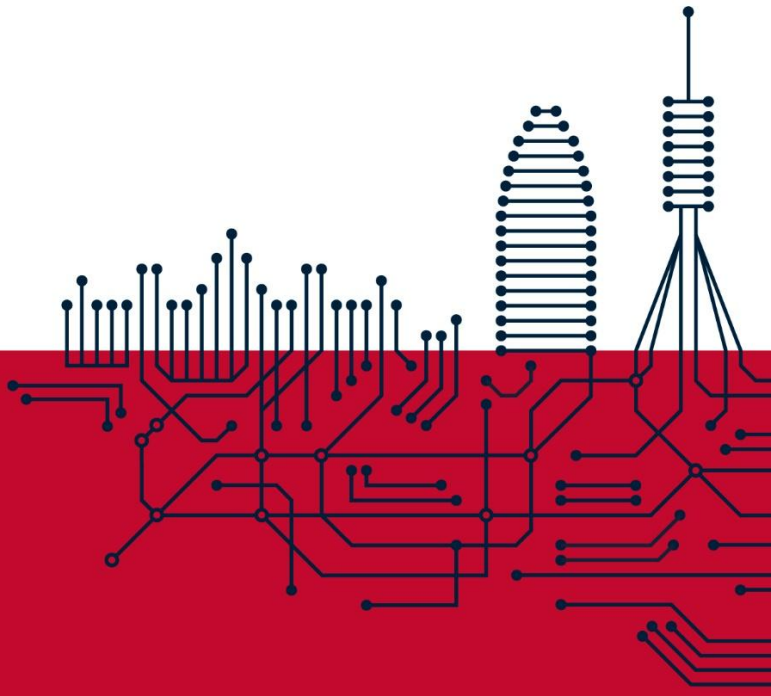
Smarting
ENGINEERING



Business Continuity Policy

SGCN.PR.01.en v1.1

06/03/2026

1. Management Statement

At **Smarting**, the continuity of critical services and organisational resilience are strategic elements to ensure the trust of our clients, partners, users and stakeholders.

The Management of **Smarting Engineering, S.L.** declares its commitment to the establishment, implementation, maintenance and continual improvement of the **Business Continuity Management System (BCMS)**, and assumes the following commitments:

1.1. Appropriate to the purpose of the organisation

- Maintain the **availability of the Motorcloud platform**, the services delivered through it and the support to clients and suppliers, as an essential activity of **Smarting**.
- Protect the ability of **Smarting** to **deliver products and services** to its clients within **acceptable timeframes** and at a **predefined capacity** during a disruption.
- Integrate continuity management into all business processes, from solution development through to operations and support.

1.2. Framework for business continuity objectives

This policy provides the framework for establishing **measurable objectives** for business continuity, including:

- **RTO** (Recovery Time Objective): target recovery time for each critical service.
- **RPO** (Recovery Point Objective): maximum acceptable data loss.
- **MTPD** (Maximum Tolerable Period of Disruption): maximum tolerable period of disruption.

Specific objectives are defined in the Business Continuity Objectives (cont.3.2), based on the results of the Business Impact Analysis (BIA, cont.5.1).

The organisation prioritises essential services and processes to ensure recovery within the established timeframes, and coordinates the response of all areas through specific plans (BCP, Emergency Protocol, Alternative Means).

1.3. Commitment to fulfil applicable requirements

Comply with all **legal, regulatory, contractual and normative requirements** applicable to business continuity, including:

- **UNE-EN ISO 22301:2020** — Business Continuity Management System.
- **ISO/IEC 27001:2022** — Information security continuity controls.
- **ENS (RD 311/2022)** — Service continuity measures (op.cont) at medium category.
- **RGPD / LOPDGDD** — Availability and recovery of personal data.
- **Contractual requirements** with clients, especially with the Autoritat del Transport Metropolità de Barcelona (ATM).

Provide the **necessary resources** for the establishment, implementation and continual improvement of the BCMS.

1.4. Commitment to continual improvement of the BCMS

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

- **Periodic tests and exercises** that validate the effectiveness of the plans.
- **Internal audits** that verify compliance with requirements.
- **Management reviews** that evaluate performance and guide decisions.
- **Nonconformity management and corrective actions** that eliminate the root causes of deviations.
- Integration of **lessons learned** from real incidents and exercises.

Promote a **culture of prevention and effective response** to incidents and disasters throughout the organisation.

Ensure the **protection of life, information and corporate reputation** in disruption scenarios.

2. Scope

This policy applies to all **processes, resources, technologies and infrastructures** of **Smarting** included in the scope of the BCMS (cont.1.3), as well as to **critical suppliers and third parties** that may impact the continuity of services.

This includes, without limitation:

- The **Motorcloud platform** and all services in production.
- The **two data centres** and associated infrastructure.
- The **operations, development, systems and support teams**.
- The **critical suppliers** of infrastructure, telecommunications and services.

3. Responsibilities

The following table summarises the responsibilities regarding this policy:

Role	Responsibility regarding this policy
Management	Approve the policy and allocate the necessary resources for its fulfilment.
CISO	Keep the policy up to date, coordinate its integration with the ISMS and disseminate it.
Security Committee	Oversee compliance with the policy and evaluate activation of the continuity plans.
Critical Area Managers	Ensure their teams are aware of and apply the policy within their area.
All employees	Know their roles within the BCP, participate in continuity training and testing, and report incidents.

4. Communication and Availability

This policy complies with the communication requirements established in ISO 22301 (5.2.2):

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.

5. Review

- This policy shall be reviewed **annually** as part of the Management Review.
- It shall be 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.
- Reviews shall be documented in the Security Committee minutes and in the Change Log (cont.3.3).

6. Relationship with the Information Security Policy

This policy complements section 16 (Business continuity) of the **Information Security Policy** (SGSI.PR.01.en) of **Smarting**. Both policies share the Security Committee governance structure and are managed in an integrated manner.

7. Approval

By approving this policy, the Management of **Smarting Engineering, S.L.** declares its determination and commitment to achieving an adequate level of resilience and operational continuity for the needs of the business, ensuring the protection of critical services, information and people in an integrated manner consistent with the ISMS.

Approved by:	Management of **Smarting Engineering, S.L.**
Date:	06/03/2026
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**