**INFORMATION SYSTEMS SECURITY POLICY**  **(ISS)**

**Brambati SpA** considers Information Systems Security (ISS) a strategic element for protecting its data, processes and relationships with customers, suppliers and stakeholders. This Policy is consistent with the principles of the European Directives NIS2 and REC, takes after the best practices of the ISO/IEC 27001 standard and integrates the requirements of the company's Integrated Management System.

**Basic principles**

The basic principles that guide information security management in **Brambati SpA** are based on:

* Availability → ensuring that systems and information are accessible and usable when required by business processes and authorised users;
* Integrity → ensuring the accuracy, completeness and reliability of data and information throughout their life cycle;
* Confidentiality → protecting information from unauthorised access, ensuring that only authorised parties can access and process it.

**Risk management**

**Brambati SpA** adopts a systematic Risk and Opportunity Analysis approach to identify, assess, and mitigate threats to information security, also considering the impact of climate change and extreme events on the continuity of ICT systems. In particular, the following are analysed:

* Cyber attacks (malware, ransomware, phishing, unauthorised access);
* Technical failures, blackouts and unavailability of critical systems;
* Natural and climatic events that can compromise infrastructure and data centres;
* Risks arising from external suppliers, partners and the digital supply chain;
* Human errors and lack of staff awareness.

Opportunities identified include:

* Adoption of innovative and secure technologies (resilient cloud, AI, blockchain);
* Developing a corporate cybersecurity culture through ongoing training;
* Increased customer and stakeholder trust through safe and reliable systems;
* Organisational resilience and rapid response capacity to incidents and crises.

**Management Commitments**

The Management of **Brambati SpA** undertakes to:

* Ensure compliance with applicable laws, regulations and directives (NIS2, REC, GDPR, Privacy Code);
* Define information security improvement objectives and programs;
* Ensure resources, roles and responsibilities for security management;
* Periodically review this Policy and the information security system to verify their effectiveness and adequacy;
* Integrate the principles of security by design and by default into the development and management of information processes and systems;
* Promote awareness and training of all staff on information security.

**Operational objectives**

The operational objectives that **Brambati SpA** poses in the SSI field include:

* Protect personal, industrial and proprietary data from unauthorised access and processing;
* Ensure business continuity and rapid recovery capabilities through Business Continuity and Disaster Recovery plans;
* Continuously monitor systems to detect and respond promptly to security incidents;
* Correctly manage access, digital identities and user privileges;
* Perform regular secure backups and restore tests;
* Evaluate and monitor critical vendors and outsourced services to ensure alignment with corporate security standards.

**Monitoring and improvement**

**Brambati SpA** ensures constant monitoring and continuous improvement of information systems security through:

* Definition and tracking of KPIs (incidents managed, average recovery times, % training completed, availability of critical systems);
* Internal and external audits to verify compliance with security policies and standards;
* Periodic threat analysis and updating of technical and organisational countermeasures;
* Active involvement of management and operational managers in decision-making processes related to the ISS.

**Integration on the use of Artificial Intelligence (AI)**

**Brambati SpA**, although it does not develop Artificial Intelligence systems, uses them in some management, production and support processes. For this reason, the company recognises the importance of ensuring that these tools are used safely, responsibly, and in compliance with European legislation, particularly the Regulation (EU) AI Act and the GDPR.

In relation to the use of AI tools, **Brambati SpA** undertakes to:

* Apply the fundamental principles of availability, integrity, and confidentiality to the data and algorithms used by AI systems;
* Assess and mitigate risks related to bias, algorithmic discrimination, and opacity of automated decisions;
* Verify AI solution providers' compliance with European regulations and industry ethical standards;
* Ensure transparency and accountability in the use of AI tools, ensuring that critical decisions are never entrusted exclusively to automated systems;
* Integrate AI into information systems’ security training, auditing, and monitoring processes.

This Information Systems Security Policy is disseminated to all personnel, made available to stakeholders, and published on the company website. It represents the formal commitment of **Brambati SpA** to protect its information assets, ensuring availability, integrity and confidentiality, and to pursue continuous improvement in IT security.

 Date **Brambati SpA** Management

Codevilla, 01/09/2025 ………………………………….