INFORMATION SECURITY POLICY
REFERENCE STANDARD: ISO/IEC 27001

Document name	INFORMATION SECURITY POLICY		
Issued by	Search Bridge s.r.l. SB		
Prepared by	ISMS Manager – Giulio Salvucci		
Approved by	Management		
Version	00	Pages	4
Date of First Issue	12/01/2026		
Classification	Public		

SUMMARY OF REVISIONS AND PREVIOUS VERSIONS

Version	Date issued	Summary of changes	Performed by
00	12/01/2026	Release	ISMS Manager – Giulio Salvucci
01	17/06/2026	Update of the scope of application	ISMS Manager – Giulio Salvucci

INDEX

1. GENERAL INTRODUCTION

Search Bridge s.r.l. is a company specialized in providing brand-perception and competitive-positioning analysis services through the use of Generative Artificial Intelligence. These services are delivered through the proprietary platform “Search Bridge”, which enables client organizations to obtain real-time strategic insights into their own brand positioning and the relevant competitive landscape, leveraging the potential of advanced language models and Generative AI technologies.

2. MANAGEMENT COMMITMENT AND OBJECTIVES

The primary objective that the Company sets for itself is the protection of data and information in order to safeguard the data of the Clients whose data it processes. Given the characteristics of the services that Search Bridge s.r.l. offers to its clients and the value that information represents within its business, the Information Security Policy represents a fundamental and priority strategic direction. The Information Security Management System is founded on compliance with:

- confidentiality: ensuring that information is accessible only to duly authorized parties within the scope of the processes managed;
- integrity: safeguarding the content and consistency of information from unauthorized modifications;
- availability: ensuring that authorized users have access to information and the associated architectural elements when they request them;
- control: ensuring that data management always takes place through secure and tested processes and tools;
- privacy: guaranteeing the protection and control of personal data and their processing.

All persons who work and/or collaborate with Search Bridge s.r.l. (including Suppliers, Clients and Partners) are committed to respecting these principles.

Search Bridge s.r.l. has defined the following objectives through the ISMS:

- to have a comprehensive and central view of corporate security, extending beyond the perimeter of IT security to also include people and processes;
- to demonstrate its ability to provide products and services that comply with client requirements, with the requirements of the reference standards, and with applicable laws and regulations;
- to increase client satisfaction through the effective application of the ISMS and of continuous-improvement processes, and by ensuring compliance with the requirements established by mandatory regulations and applicable rules.

3. THE INFORMATION SECURITY MANAGEMENT SYSTEM

Search Bridge s.r.l. has always been committed to applying the principles of Privacy by Design and Privacy by Default in the design, management and maintenance of its technological, physical, logical and organizational structure.

Search Bridge s.r.l. believes that information security represents a decisive success factor both with regard to the processes of design and development of technological solutions and with regard to the delivery of services.

The information security policy consists of a set of activities that include: the identification of critical areas; the management of risks, systems and the network, of vulnerabilities and incidents; access control; the management of privacy and compliance; the assessment of damages and all other aspects that may impact the management of information security.

The governing body is strongly committed to a high level of accountability of all the people who work for and with the company in ensuring the rigor of their conduct in order to fulfill, with the utmost attention, the tasks assigned to them. In particular, this objective is pursued through the commitment to guarantee:

1. compliance with applicable laws and regulations;

2. the operational efficiency and reliability of the processes for developing related products and services;

3. health and safety conditions in the workplace for personnel and third parties;

4. the continuity and efficiency of organizational and operational processes in order to prevent and minimize the impact of intentional or accidental incidents on the security of the data/information managed;

5. the protection of the tools made available and their proper use;

6. the confidentiality, correctness and availability of the data/information managed by Search Bridge s.r.l. and the safeguarding of intellectual property;

7. the adoption of measures to prevent process/product/service anomalies.

To implement its information security policy, Search Bridge s.r.l. has developed, and is committed to maintaining, a secure information management system compliant with the specified requirements, with the UNI CEI EN ISO/IEC 27001 standards and with mandatory laws, as a means to manage information security within the scope of its activity. In managing the services offered, the organization ensures:

- observance of the security levels established through the implementation of the ISMS (information security management system);
- compliance with applicable regulations and international security standards for its technological and organizational infrastructure;
- the selection of partners that are reliable in terms of secure information management and personal data protection.

3.1. SCOPE OF APPLICATION

This policy applies without distinction to all bodies and levels of the Company. Implementation of this policy is mandatory for all personnel and must be incorporated into the regulation of agreements with any external party that, in any capacity, may be involved in the processing of information falling within the scope of the Management System (ISMS): the scope of application is:

“Design, development, delivery and maintenance of a cloud platform (SaaS) for the analysis of brand reputation in search systems, based on artificial intelligence models”.

In addition to internal personnel, the information security policy also applies to third parties that collaborate/participate in the processes and to the resources involved in the design, implementation, start-up and ongoing delivery within the scope of the services.

The commitment extends to the internal organization and to stakeholders. The ISP represents, in concrete terms, the organization’s commitment to clients and third parties to guarantee the security of information and of the physical, logistical and organizational tools used for the processing of information in all activities.

4. STATEMENT OF COMMITMENT

In summary, the information security policy guarantees:

a) that the organization has full knowledge of the information managed and assesses its criticality on a case-by-case basis, in order to facilitate the implementation of adequate levels of protection;

b) that access to information takes place in a secure manner, suitable to prevent unauthorized processing or processing carried out without the necessary rights;

c) that the organization and third parties collaborate in the processing of information by adopting procedures aimed at complying with adequate levels of security;

d) that the organization and the third parties that collaborate in the processing of information are adequately trained and have full awareness of the issues relating to security;

e) that anomalies and incidents having repercussions on the IT system, on the services and on the corporate security levels are promptly recognized and correctly managed through

efficient systems of prevention, communication and response, in order to minimize the impact on the business;

f) that access to the premises and to the individual company rooms takes place exclusively by authorized personnel, to guarantee the security of the areas and of the assets present;

g) compliance with legal requirements and adherence to the security commitments established in contracts with third parties;

h) that the detection of anomalous events, incidents and vulnerabilities of the information systems is correctly carried out, in order to ensure the security and availability of the services and of the information;

i) business continuity;

l) that the processing of personal data, both in cases where Search Bridge s.r.l. acts as Data Controller and in cases where it operates on behalf of third parties as Data Processor, takes place in compliance with the European Regulation on the Protection of Personal Data, GDPR 679/2016.

The information security policy is constantly updated and verified during the annual review of the ISMS, as well as whenever contingent conditions arise that create new opportunities, in order to ensure its continuous improvement. It is therefore shared with the organization, third parties and clients.

5. RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION

Compliance with, and implementation of, the policies are the responsibility of:

1. all personnel who, in any capacity, collaborate with the company and are in any way involved in the processing of data and information falling within the scope of the Management System. All personnel are also responsible for reporting any anomalies and violations of which they become aware.

2. All external parties that maintain relationships and collaborate with the company must ensure compliance with the requirements contained in this policy. The Information Security Management System Manager who, within the scope of the Management System and through appropriate rules and procedures, must: conduct the risk analysis using appropriate methodologies and adopt all measures for risk management

2. establish all the rules necessary for the safe conduct of all company activities

3. verify security violations and adopt the necessary countermeasures, and monitor the company’s exposure to the main threats and risks

4. organize training and promote personnel awareness of everything concerning information security.

5. periodically verify the effectiveness and efficiency of the Management System.

Anyone — employees, consultants and/or external collaborators of the Company — who, intentionally or through negligence, disregards the established security rules and thereby causes damage to the company, may be prosecuted in the appropriate legal forums and in full compliance with legal and contractual constraints.

6. REVIEW

The Governing Body will periodically and regularly, or in conjunction with significant changes, verify the effectiveness and efficiency of the Management System, so as to ensure adequate support for the introduction of all necessary improvements and so as to foster the activation of a continuous process, through which control and adjustment of the policy are maintained in response to changes in the corporate environment, the business and legal conditions.

The review shall verify the status of preventive and corrective actions and adherence to the policy.

It shall take into account all changes that may influence the company’s approach to information security management, including organizational changes, the technical environment, the availability of resources, legal, regulatory or contractual conditions, and the results of previous reviews.

The result of the review shall include all decisions and actions relating to the improvement of the company’s approach to information security management.

Management
Search Bridge s.r.l.

Giulio.salvucci

Signed by GIULIO SALVUCCI
Date: 03/07/2026 at 09:21:58 UTC