

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 1 of 7

INFORMATION SECURITY POLICY

REFERENCE STANDARD: ISO/IEC 27001

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 2 of 7

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

REVISION SUMMARY AND PREVIOUS VERSIONS

Version	Issue date	Summary of changes	Performed by
00	12/01/2026	Release	Giuli

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 3 of 7

INDEX

1. GENERAL PREAMBLE	4
2. MANAGEMENT COMMITMENT AND OBJECTIVES	4
3. THE INFORMATION SECURITY MANAGEMENT SYSTEM	5
3.1. SCOPE OF APPLICATION	6
4. STATEMENT OF COMMITMENT	7
5. RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION	8
6. MANAGEMENT REVIEW	9

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 4 of 7

1. GENERAL PREAMBLE

Search Bridge s.r.l. is a company specialised in the provision of brand perception analysis and competitive positioning services through the use of Generative Artificial Intelligence. These services are delivered through the proprietary platform "Search Bridge", which enables client organisations to obtain real-time strategic insights into their brand positioning and the competitive landscape of reference, leveraging the capabilities of advanced language models and Generative AI technologies.

2. MANAGEMENT COMMITMENT AND OBJECTIVES

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

- **confidentiality**: ensuring that information is accessible only to duly authorised parties within the managed processes;
- **integrity**: safeguarding the content and consistency of information from unauthorised modifications;
- **availability**: ensuring that authorised users have access to information and the associated architectural elements, when requested;
- **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, through the ISMS, the following objectives:

- to have an overall and centralised view of corporate security, extending beyond the IT security perimeter to also include people and processes;
- to demonstrate its ability to provide products and services that comply with client requirements, the requirements of reference standards, applicable laws and regulations;
- to increase client satisfaction through the effective application of the ISMS and 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 organisational structure.

Search Bridge s.r.l. considers information security to be a decisive success factor both in relation to the processes of designing and developing technological solutions and in relation to service delivery.

The information security policy consists of a set of activities that include: the identification of critical areas; risk management, systems and network management, vulnerability and incident management; access control;

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 5 of 7

privacy and compliance management; damage assessment and all other aspects that may impact information security management. The governing body is strongly committed to a high degree of accountability from all persons who work for and with the company, ensuring the rigour of their conduct in fulfilling, with the utmost care, the tasks assigned to them. In particular, this objective is pursued through the commitment to guarantee:

1. compliance with applicable laws and regulations;
2. operational efficiency and reliability of the product and service development processes;
3. health and safety conditions in the workplace for personnel and third parties;
4. the continuity and efficiency of organisational and operational processes in order to prevent and minimise the impact of voluntary or accidental incidents on the security of managed data/information;
5. the protection of the tools made available and their correct use;
6. the confidentiality, correctness and availability of 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.

In order to implement its information security policy, Search Bridge s.r.l. has developed and commits to maintaining a secure information management system compliant with the specified requirements of UNI CEI EN ISO/IEC 27001 standards and applicable mandatory laws, as a means of managing information security within its operations. In the context of managing the services offered, the organisation ensures:

- compliance with the security levels established through the ISMS (information security management system) implementation;
- adherence to applicable regulations and international security standards for its technological and organisational infrastructure;
- the selection of reliable partners 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:

"Provision of brand perception analysis and competitive positioning services, including through the use of Generative Artificial Intelligence".

In addition to internal personnel, the information security policy also applies to third parties that collaborate in/intervene in processes and to resources involved in the design, implementation, launch and ongoing delivery of services.

The commitment extends to the internal organisation and to stakeholders. The ISP concretely represents the organisation's commitment to clients and third parties to guarantee the security of information, and of the physical, logistical and organisational tools used for the processing of information in all activities.

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 6 of 7

4. STATEMENT OF COMMITMENT

In summary, the information security policy guarantees:

- a) that the organisation has full knowledge of the information it manages and assesses, on a case-by-case basis, its criticality, in order to facilitate the implementation of adequate levels of protection;
- b) that access to information takes place in a secure manner suited to preventing unauthorised processing or processing carried out without the necessary rights;
- c) that the organisation and third parties collaborate in the processing of information by adopting procedures aimed at respecting adequate security levels;
- d) that the organisation and third parties collaborating in the processing of information are adequately trained and have full awareness of security-related issues;
- e) that anomalies and incidents affecting the IT system, services and corporate security levels are promptly identified and correctly managed through efficient prevention, communication and response systems, in order to minimise the impact on business;
- f) that access to the company premises and individual offices takes place exclusively by authorised personnel, guaranteeing the security of the areas and assets present;
- g) compliance with legal requirements and respect for the security commitments established in contracts with third parties;
- h) that the detection of anomalous events, incidents and vulnerabilities in information systems is carried out correctly, in order to maintain the security and availability of services and 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 acts on behalf of third parties as Data Processor, takes place in compliance with the European General Data Protection Regulation GDPR 679/2016.

The information security policy is constantly updated and verified, during the annual ISMS review and also whenever contingent conditions arise that determine new opportunities, in order to ensure its continuous improvement. It is therefore shared with the organisation, 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 all anomalies and violations that come to their attention.
2. All external parties that maintain relations and collaborate with the company must guarantee compliance with the requirements contained in this policy. The Information Security Management System Manager, within the scope of the Management System and through appropriate rules and procedures, must:
 1. conduct risk analysis using appropriate methodologies and adopt all measures for risk management;
 2. establish all rules necessary for the secure conduct of all corporate activities;

3. verify security breaches and adopt the necessary countermeasures, and monitor the company's exposure to major threats and risks;
4. organise training and promote staff awareness on all matters relating to information security;
5. periodically verify the effectiveness and efficiency of the Management System.

SEARCH BRIDGE	Search Bridge s.r.l. Via Del Giacinto n. 32, 40133 Bologna (BO),	12/01/2026 Rev. 00
	INFORMATION SECURITY POLICY	PAG 7 of 7

Any employee, consultant and/or external collaborator of the Company who, intentionally or through negligence, fails to comply with the established security rules and thereby causes damage to the company, may be prosecuted in the appropriate venues and in full compliance with legal and contractual constraints.

6. MANAGEMENT REVIEW

The Governing Body shall periodically and regularly verify, or verify in conjunction with significant changes, 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 promote the activation of a continuous process, through which control of and adaptation to the policy is maintained in response to changes in the corporate environment, 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 organisational changes, the technical environment, resource availability, legal, regulatory or contractual conditions, and the results of previous reviews.

The outcome of the review shall include all decisions and actions relating to the improvement of the corporate approach to information security management.

The Management

Search Bridge s.r.l.

Giulio.salvucci

Signed by GIULIO SALVUCCI
Date: 08/03/2026
at 15:52:20 UTC