POL Management System Policy

Version history

Version	Date	Author	Approved by
1	28/04/2026	Anton Morale	Matteo Trovò

Contents

Purpose

StepsConnect regards information security as a cornerstone of its business strategy. Founded in 2019 with the mission of modernising high-volume recruitment processes through artificial intelligence, the organisation places the protection of candidate data, client information and the source code of its cloud platform at the centre of every operational and development decision.

With this policy, **Top Management** sets out the principles, commitments and direction that guide the Information Security Management System (ISMS), so that it is appropriate to the organisational context, the business model and the expectations of interested parties. The organisation promotes an approach in which economic growth, technological innovation and value creation are integrated with the protection of information assets, full compliance with applicable legislation and the spread of a security culture at every level. This policy is the high-level reference that informs the entire body of ISMS documentation, starting with the *POL Information Security Policy*, which translates its principles into a detailed operational framework, and the related procedures.

Scope

This policy applies to all activities of design, development, delivery and support of software solutions and artificial intelligence and process automation technologies for the search, selection and management of human resources carried out by StepsConnect. The scope covers all information assets, organisational processes, technology systems and the cloud infrastructure on which the platform runs. The policy extends to all personnel (employees, contractors and third parties who access company information or systems), regardless of their place of work, including the registered office at Via Luigi Galvani 24, 15121 Alessandria and remote workstations.

Normative references

- ISO/IEC 27001:2022
- Regulation (EU) 2016/679
- Italian Legislative Decree 196/2003

Terms and definitions

- **Information Security Management System (ISMS):** part of the overall management system, based on a risk-based approach, to establish, implement, maintain and improve information security.
- **Information security:** preservation of the confidentiality, integrity and availability of information.
- **Confidentiality:** property that information is not made available or disclosed to unauthorised individuals, entities or processes.
- **Integrity:** property of accuracy and completeness of information.
- **Availability:** property of being accessible and usable on demand by an authorised entity.
- **Risk:** effect of uncertainty on objectives.
- **Interested party:** person or organisation that can affect, be affected by, or perceive itself to be affected by a decision or activity.
- **Continual improvement:** recurring activity to enhance performance.
- **Policy:** intentions and direction of an organisation, as formally expressed by its top management.
- **Documented information:** information required to be controlled and maintained by an organisation and the medium on which it is contained.

Roles and responsibilities

- **Top Management:** approves this policy, verifies its adequacy during the management review and ensures it is communicated at all levels of the organisation and to relevant interested parties.
- **Management System Manager:** drafts, updates and disseminates this policy, monitoring its application and proposing the necessary revisions based on the organisational context, audit results and risk assessments.

Management system commitment and objectives

Organisational commitments

StepsConnect takes an approach to information security based on the systematic assessment of risks, recognising that protecting information assets is a responsibility shared by every level of the organisation. **Top Management** is committed to providing the resources needed to achieve security objectives and to fostering a culture in which safeguarding information is an integral part of all personnel's daily activities.

The organisation seeks to preserve the confidentiality, integrity and availability of the information it processes, with particular attention to the personal data of candidates and clients, the platform's source code and any other asset relevant to service continuity. StepsConnect recognises the value of complying with applicable legal, regulatory and contractual requirements and promotes adherence to personal data protection and cybersecurity rules, supported by a designated DPO and by constant monitoring of changes in the legislative framework.

Information security risk management is based on a structured process of identification, assessment and treatment, governed by the *PRO Risk Management Procedure*. The process defines probability and impact scales, a tolerance threshold above which every risk is treated, and periodic reassessment, as well as reassessment whenever significant changes occur in the internal or external context, as documented in the *Context Analysis*.

StepsConnect integrates security into every phase of the software development lifecycle, from design to production release, adopting secure development principles and environment segregation in accordance with the *PRO Secure Development Procedure*. The fully cloud-based infrastructure on which the platform runs also requires careful management of relationships with ICT service providers: the organisation assesses the security and compliance implications of outsourced services and monitors their service levels through the processes defined in the *PRO Procurement and Third-Party Management Procedure*.

The organisation promotes personnel awareness and competence in information security through training and awareness programmes tailored to assigned roles and responsibilities, so that every team member can promptly recognise and report anomalous events or potential vulnerabilities. StepsConnect protects those who make reports in good faith and considers everyone's active contribution essential to the effectiveness of security controls.

Ensuring business continuity and the ability to restore critical services in the event of adverse events is a further commitment of the organisation, pursued by defining measurable recovery objectives and preparing continuity and disaster recovery plans, as described in the *PRO Business Continuity and Disaster Recovery Procedure*.

Top Management is committed to the continual improvement of the ISMS, drawing on the results of internal audits, risk assessments, performance indicators and evidence from the management review to continually refine security controls and processes.

Information security objectives

StepsConnect sets information security objectives consistent with this policy and with the company's strategic direction. Objectives are measurable, communicated to the relevant functions and periodically reviewed during the management review, as provided for in the *PRO Management Review Procedure*. The objectives are organised along the following lines:

- preserve the confidentiality, integrity and availability of the information managed by the platform and by business processes, with specific attention to personal data and source code;
- ensure compliance with applicable legal, regulatory and contractual requirements, particularly with regard to personal data protection;
- manage information security risks through a systematic and documented process, treating every risk that reaches or exceeds the tolerance threshold set by the organisation;
- ensure the resilience of critical services by pursuing defined and verified recovery objectives;
- develop and maintain personnel competence in information security through training tailored to roles and responsibilities;
- integrate security into the software development lifecycle, from design to production release.

The **Management System Manager** monitors the achievement of objectives through defined indicators and reports to **Top Management** at the management review, proposing the necessary improvement actions. **Top Management** evaluates the results achieved and, where necessary, redefines objectives and priorities for the following cycle, ensuring a cyclical process of planning, implementation, checking and improvement.

Retention and updates

This policy is retained as ISMS documented information and made available to all personnel through the approved company communication channels, in accordance with the *PRO Communication Management Procedure*. Internal distribution takes place via company email, document-sharing platforms, company messaging, team meetings and training sessions; each recipient signs an acknowledgement of receipt. The policy is also published on the public pages of the company website, placed in the footer so that anyone visiting can view and download it, and made available to clients and suppliers through contractual documentation.

The policy is reviewed at least at every management review, and following significant changes to the organisational context, strategic direction, or the results of risk assessments or audits, as governed by the *PRO Management Processes Procedure*. The **Management System Manager** prepares the draft update, which **Top Management** reviews and formally approves. Every change is recorded in the revision log, versioned and communicated to all personnel and relevant interested parties through the approved channels. Superseded versions are archived with their replacement date and made unavailable for current operational use.

Reference documents

- POL Information Security Policy
- PRO Risk Management Procedure
- PRO Secure Development Procedure
- PRO Procurement and Third-Party Management Procedure
- PRO Business Continuity and Disaster Recovery Procedure
- PRO Management Review Procedure
- PRO Management Processes Procedure
- PRO Communication Management Procedure
- Context Analysis