Fullstep
Optimizamos sus costes

Security Policy
December 2018

Owner:
Antonio Fernandez Ruiz
Technology Director

Contents

1 Introduction

The business processes in Fullstep depend largely on the Information Systems and the information they store. The purpose of this Policy is to establish the global security guidelines for the organization, and to protect the information assets.

These directives entail the adoption of a series of organizational measures and standards included in this document and explained further in the associated documents, the purpose of which is to protect Fullstep's information assets and the information systems used to process it from internal and external threats, whether intentional or accidental, so as to guarantee that the information is fully compliant in terms of confidentiality, integrity, availability and legality.

This policy is based on the recommendations of the best practices to guarantee Security in Information System Management (International standards ISO 27001 and ISO 27002) and all applicable legislation on this matter.

2 Purpose

The main purpose in creating this Policy is to guarantee user access to the information in the amount and quality that they need for their work, and to prevent serious loss of information or unauthorized access to it.

3 Information security policy

In response to a new technological environment in which the convergence of IT and communications is creating a new paradigm for productivity in business, Fullstep is fully committed to offering its consultancy services and support for purchasing and development and the implementation of purchasing management systems in a quality environment where the use of good security practices is essential to achieve the objectives of confidentiality, integrity, availability and legality for all the information managed for the progress of Fullstep.

Fullstep, therefore, defines the following guidelines to be taken into account:

Confidentiality: Information processed by Fullstep will only be known by authorized persons, subject to identification at the time and using the established means.

- **Integrity:** The information processed by Fullstep shall be complete, precise and valid, its content submitted by those involved without manipulation of any kind.
- **Availability:** The information processed by Fullstep will be accessible and available for authorized and identified users at all times, and its permanence is guaranteed despite any expected eventuality.
- **Legality:** Fullstep guarantees compliance with all applicable legislation. Specifically, all current law in relation with the processing of personal data.

With this policy, the Senior Management assumes responsibility for supporting and promoting the establishment of the organizational, technical and control measures required to comply with the security directives listed here. The Security Policy will therefore be upheld, updated and adjusted to the needs of the organization, in alignment with its risk management environment. There will therefore be reviews at regular intervals, or when significant changes occur, to ensure that its suitability, adequacy and effectiveness is maintained. All changes and modifications will be approved and promoted by Fullstep Senior Management.

4 Scope

4.1 Employees

Information security is the result of collective effort. It demands the involvement and participation of all members of the organization who work with the information systems. Every employee must therefore satisfy the requirements of the Security Policy and its associated documents. Disciplinary measures will be taken against employees who deliberately or negligently break the Security Policy, as described in the last chapter of this document.

4.2 Information systems

This policy affects all information assets of the company, whether on paper or manual, personal or otherwise, stored on personal devices or servers, networks, applications, operating systems, company policies that belong to and/or are administered by Fullstep. This policy covers the aspects most closely related with responsibility and good use by personnel.

4.3 Third parties

Knowledge and compliance of this Security Policy shall extend to any external person employed by third parties who carry out any type of processing of the information belonging to Fullstep. Compliance of this policy and its associated procedures shall be mandatory for the third party companies employed to perform professional services in any area considered appropriate, should they perform any activity that relies on access or processing of any system or information belonging to Fullstep, and this shall be reflected in the contract.

5 Roles and responsibilities

5.1 Users

Users must know and apply the Security Policies, procedures, standards as well as the current legislation. They must understand and comply with them.

In general, any person who creates information is responsible for classifying it in accordance with the Company's instructions. Likewise, any person who uses information and information systems

is required to handle them with due care and to use them only for the tasks for which they are authorized and in accordance with the law. This also applies to external personnel.

5.2 Owners

The ownership of the information assets generally corresponds to the Senior Management or Area Supervisors, who must acquire, develop and maintain Company applications as support systems for the decisions and other activities.

The owners must indicate the classification of their assets that best corresponds to their critical value, availability and relative importance for the organization. This classification will indicate the level of risk and protection, as well as the level of access to this information or application.

5.3 Administrators

The administrators are employees responsible for ensuring the security of the Company's own information and that, transferred by third parties.

Each information system must have at least one authorized Administrator as stated in the Security Document.

They are responsible for storing the information, implementing access controls (to prevent unauthorized access) and make regular security copies (to ensure the availability of critical information).

6 Policy maintenance, approval and review

The Information Security Supervisor is responsible for establishing and maintaining the Security Policy, manuals and procedures for Fullstep.

The company's Senior Management is responsible for approving and publishing the Policy, distributing it to all affected employees and third parties, as well as reviewing and evaluating the Security Policy.

Any change of development that affects or may affect the content of this Security Policy will be registered in a new signing of the approval document. This will manifest and confirm the commitment to information security.

The validity and suitability of this Policy will be revised regularly, in no case in a period of more than one year, and any improvements, adaptations or modifications required by organizational, technical or regulatory changes will be carried out.

7 Policy distribution

All internal personnel will have access to the Security Policy document, which will be given to new employees on induction and distributed every year by email and the corporate tool "https://wiki.fullstep.net/" to all internal employees and external personnel subcontracted by

Fullstep who handle its data and resources so that they know and are aware of the security regulations it contains.

All the employees will commit to reading and accepting it.

Any substantial change in the document shall be distributed to all users through a formal notification, sent by email or internal communication on accessible media made possible by a communication model set up for this purpose.

8 Penalties

Any intentional breach or negligence of the security policies and regulations that represent a potential loss to Fullstep, whether actual or not, shall be penalized in accordance with the terms stated in the applicable Company regulations and contracts and the law.

Any action that may compromise the security of Fullstep and which is not foreseen in this Policy shall be revised by the Senior Management and Security Supervisor in order to issue a decision subject to the criteria of the Company and legislation.

Disciplinary actions in response to any breaches of the Security Policy are the responsibility of the Departmental Supervisors in agreement with the Administration and Senior Management.

In Madrid, December 19 2018

Antonio Fernandez Ruiz

Technology Director