SOL GROUP COMPANIES POLICY REGARDING INFORMATION SECURITY AND BUSINESS CONTINUITY

Introduction

The success factors of the SOL Group strategy are:

- the business internationalization to compete on a global market;
- the ability to anticipate the changing needs of the application;
- diversification and development of new market opportunities;
- customer orientation;
- continuous improvement and innovation of product and service, increasingly seen as a commitment to providing solutions "tailor made".

Having regard to the strategic importance lies in the management of information security and business continuity, networks and IT systems for their own business, the SOL Group adopts a policy suited to current and future needs.

SOL is aware that the management of information security and business continuity is a complex cultural process that must involve, at all levels and so pervasive, the individual operations of all the human resources allocated to all organizational units within the scope of certification perimeter (hereinafter referred to as "scope").

Goals

To enable the SOL Group to develop and consolidate its leadership position in the markets, it is necessary to ensure:

- the drawing, updating and monitoring of development plans to ensure that the infrastructure and IT services support business activities, taking appropriate security policies;
- the quality and reliability of IT services delivered;
- the safe storage of managed information;
- the continuity of IT services delivered based on business needs.

SOL recognizes the need to develop, maintain, monitor and improve constantly the information security and business continuity Management System (hereinafter referred to as ISMS and BCMS) in compliance with ISO/IEC 27001, extended in compliance with ISO 27017 and ISO/IEC 27018 guidelines, and ISO 22301 and with the General Data Protection Regulation (GDPR).

The ISMS and BCMS are realized by ensuring:

- the confidentiality of managed information assets, assets made available only to authorized individuals and / or entities;
- the integrity of managed information assets, protecting property, reliability and completeness;
- the availability of managed information assets, which must be accessible and usable by authorized entities;
- the business continuity of IT services delivered

through:

- compliance with the mandatory requirements of the regulatory framework and contractual obligations;
- compliance with privacy requirements of laws (GDPR, D.Lgs. 101/2018, etc.), standard (ISO/IEC 27018, etc.) and contractual requirements;

- the appropriate definition of the security requirements shared with customers of cloud services, in accordance with ISO / IEC 27017;
- adequate training in the field of staff safety information;
- the effectiveness and efficiency of control measures to avoid, deter, manage, and track, actions and / or events that may violate the safety information.

The implementation of the ISMS and BCMS is to:

- identified within the Integrated Management System, a methodology for risks assessment from the management of requested information and business requirements; according to this method to identify the threats to which these information may be subject;
- bring risks to an acceptable level, in line with organization's risk management strategies;
- to define and apply the operational guidelines, rules, functions, tools, objects and controls, which ensure in any organizational structure, IT environment, single processor, compliance with the standards defined by SOL;
- control, taking every hint of improvement, the system implemented;
- ensure compliance with the security requirements for cloud services agreed with customers.

Application

The Policy for information security and business continuity is applied to all SOL employees, to the partner companies, to suppliers, customers or third party under temporary or permanent contract, involved in the treatment of corporate information assets in the field or who has access to the premises field.

Responsibility

This policy is issued and reviewed by SOL Group top management.

The ISMS and BCMS Responsible, appointed by top management facilitates the implementation of this policy through appropriate rules and procedures. All staff and suppliers must follow the procedures established by policy of information security and business continuity.

All employees in the certification scope, according to their knowledge, has the responsibility to report to the ISMS and BCMS Responsible any weaknesses identified. Any action that intentionally causes or may cause damage to SOL, should be pursued in the proper seat.

Review

This policy is reviewed annually during the QSGC and whenever there is a need due to the implementation of changes relating to it, to make sure it remains appropriate to the aims of the SOL Group, the expectations of the users and all interested parties.

Chairman

(Aldo Rumagalli Romario)

General Managers

(Giulio Mario Bottes - Andrea Monti)

Quality, Safety, Environmental and Regulatory Affairs Director

(Daniele Valtolina)

May 2020

SOLGROUP
a breath of life