Policy on the Information Security and

Privacy Management System (ISMS)

Exprivia's information security policy requires, in coherence with the company mission, the management of all its business processes to be based upon its rules of application of the ISO/IEC 27001 standard and the regulatory requirements contained in Italian Legislative Decree 196/03 and EU Reg. 679/2016. The principle is that what is laid down by existing legislation on personal data protection are technical and organisational security measures and that personal data are a subset of information that must be protected, not only for the company business but also to respect the rights and freedoms of natural persons.

Furthermore, Exprivia, in providing ICT cloud solutions, considers the need to extend the scope of information security by following the ISO/IEC 27017 “Code of practice for information security controls based on ISO/IEC 27002 for cloud services” and ISO/IEC 27018 “Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors” Guidelines.

Purpose

The Management of Exprivia has defined and disseminated at all levels of its organisation this policy on the Information Security and Privacy Management System.

The purpose of this policy is to guarantee protection from all threats, internal or external, intentional or accidental:

- the information necessary for Exprivia's business (of which personal data is just one of the classes of information to be protected),
- the information of its clients which is managed in the life cycle of products and services supplied to the same

in conformity with the indications envisaged by Italian Legislative Decree 196/03, EU Reg. 679/2016, ISO/IEC 27001 and the ISO/IEC 27017 and ISO/IEC 27018 Guidelines.

Scope of application

This policy applies without distinction to all the bodies and levels of Exprivia.

It is mandatory for all the personnel to implement this policy and it must be communicated to any external party who, for any reason, may be involved in processing information that falls within the scope of application of the Information Security Management System.

Our policy on Information Security

The information assets to be protected are composed by the set of information managed through the services provided and localised in all offices of the company.

It is necessary to guarantee:

- the confidentiality of the information: namely, the information must only be accessible to authorised persons.
- the integrity of the information: namely to protect the correctness and completeness of the information and the methods of its processing.

- the availability of the information: namely that authorised users can actually access the information and the assets that contain it.

The absence of adequate security levels may lead to damage being caused to the company image, a lack of customer satisfaction, the risk of incurring sanctions linked to the violation of laws and regulations in force as well as damage of an economic and financial nature.

An adequate level of security is also essential for sharing information.

The company also identifies all security requirements by analysing and assessing the risk to information security and through the DPIA (Data Protection Impact Assessment) on the protection of personal data through which knowledge is gained on the level of exposure to threats of the data management system.

The risk assessment and the DPIA allow for an assessment of the potential consequences and damages, material and immaterial, that may derive from any failure to apply the technical and organisational security measures to the information assets and the probability of occurrence of the identified threats.

The results of this assessment determine the necessary actions to identify the correct and adequate security measures and mechanisms to guarantee personal data protection.

Responsibility for compliance and implementation

Compliance with and implementation of the policy are the responsibility of all personnel and all external parties who hold relationships or collaborate with Exprivia, and who are in any way involved in the processing of data and information that falls within the scope of application of the Information Security and Privacy Management System. Everyone is also responsible for reporting any anomalies and violations of which they become aware.

Anyone - employees, consultants and/or external collaborators of the Company - who, intentionally or negligently, disregards the established security rules, causing damage to Exprivia, may be prosecuted in the appropriate venues and in full respect of legal and contractual rules.

Review

Management verifies periodically and regularly the effectiveness and efficiency of the Information Security and Privacy Management System, so as to promote and encourage the activation of a continuous improvement process, also in response to changes in the internal and external environment.

Management commitment

Management actively supports activities relating to the management of information security and privacy by way of clear guidance, a strong commitment, explicit assignments and recognition of responsibilities in the field of information security and privacy.

Management's commitment is implemented through a structure the duties of which are:

- to guarantee that all objectives relating to information security and privacy, as well as conformity with the business requirements, are identified;
- to establish the company roles and responsibilities for developing and maintaining the ISMS;
- to provide sufficient resources for the planning, implementation, organisation, control, revision, management and continuous improvement of the ISMS;

- to check that the ISMS is integrated into all business processes and that procedures and controls are effectively developed;
- to approve and support all initiatives aimed at improving information security and privacy;
- to activate programmes for spreading awareness and a culture of information security and privacy.

Molfetta, 11/12/2013

Il Chairman & CEO

Dott. Domenico Favuzzi