Information Security Policy

AQAIA CONSULTING is a software engineering company, specializing in the implementation of custom solutions based on Office 365, mobility and .NET. As software developers we are aware that information is a key asset that has a high value for any organization and therefore requires adequate protection, so we have decided to implement an **Information Security Management System** (ISMS) in order to protect it from threats and intended to ensure continuity of business lines, minimize damage and maximize return on investment and business opportunities.

The management of **AQAIA** defines the security of information as the preservation of the three fundamental characteristics:

- **Confidentiality**, ensuring that only those who are authorized can access the information.
- Its **integrity**, ensuring that the information is not altered during storage, treatment or transit.
- **Availability**, ensuring that authorized users have access to information and their associated assets when required.

The management of **AQAIA** establishes as base objectives, starting point and support of the objectives and principles of the security of the information the following ones:

- The protection of personal data and the intimacy of people.
- The protection of intellectual and industrial property rights.
- The establishment of an information classification system to safeguard the records of the organization.
- The assignment of security responsibilities.
- The training for information security.
- The recording of security incidents and their lessons learned.
- The management of business continuity.
- The compliance with legislation and other regulations in force in the field of security.
- Ensuring the confidentiality, integrity and availability of the information supported by the services covered by this system.

The management of **AQAIA**, through the elaboration and implementation of this Information Security Management System acquires the following commitments:

- Objectives are established annually in relation to information security.
- A process of risk analysis is developed and according to its result, the corresponding actions are implemented in order to deal with the risks that are considered unacceptable.
- Control objectives are set based on the risk requirements arising from the managed risk analysis process.
- Compliance with business, legal or regulatory requirements and contractual security obligations.
- Provide information security awareness and training to all staff.
- To promote and support the implementation of the necessary measures to minimize the risks to which the information is exposed in the achievement of the strategic objectives that are defined year by year.

- Business continuity management, developing continuity plans according to methodologies of recognized international prestige.
- Act at all times within the strictest professional ethics.

This policy provides the framework for the continuous improvement of the Information Security Management System as well as to establish and review the objectives of the Information Security Management System, being communicated to the entire organization, being reviewed annually for its adequacy and extraordinarily when concurring special situations and/or substantial changes in the Information Security Management System, being available to the general public.

In Barcelona at 31st May 2019

Lleonard del Río
Manager & CISO