Sede legale e sede operativa:
Centro Direzionale Milanofiori
Strada 2 – Palazzo C3 - 20057 Assago (MI) Italy
Tel +39.02.82450311 – Fax +39.02.57512632
E-mail: info@azcomtech.com - Web: www.azcomtech.com
Partita IVA: 11723250152

Information Security Management System Policy

1 Scope

The purpose of this document is to describe the general information security principles defined by Azcom Technology in order to develop an efficient and secure Information Security Management System.

2 Description

For Azcom Technology the information security has as its primary objective the protection of data and information and the technological, physical, logical and organizational structure for their management. This means obtaining and maintaining a secure information management system, within the scope defined for the ISMS, by respecting the following principles:
1. Confidentiality: ensure that information is accessible only to duly authorized persons and / or processes;
2. Integrity: safeguarding the consistency of the information from unauthorized changes;
3. Availability: ensure that authorized users have access to information and associated architectural elements when requested;
4. Control: ensure that data management always takes place through safe and tested processes and tools;
5. Authenticity: guaranteeing a reliable source of information;
6. Privacy: guarantee the protection and control of personal data.

As part of the management of the services offered by Azcom Technology, through its technological infrastructure, the compliance with the security levels established through the implementation of the ISMS ensures:
- the guarantee of having appointed a reliable partner to process its information assets;
- a high corporate image;
- full compliance with the Service Level Agreements established with customers;
- customer satisfaction;
- compliance with current regulations and international safety standards.

For this reason, Azcom Technology has developed a secure information management system following the specified requirements of the ISO 27001: 2013 standard and mandatory laws as a means of managing information security as part of its business.

3 Application

Azcom Technology's information security policy applies to all internal staff and third parties who collaborate in the area of information management and to all processes and resources involved in the design, implementation, start-up and continuous provision of services.
The information security policy is available in both paper and electronic format and is communicated within the organization and to all stakeholders.

4 Information Security Policy

Azcom Technology's security policy represents the organization's commitment to customers and third parties to ensure the security of information, physical, logical and organizational tools for processing information in all activities.
Azcom Technology's information security policy is inspired by the following principles:

a) Guarantee the organization full knowledge of the information managed and the assessment of their criticality, in order to facilitate the implementation of adequate levels of protection;

b) Ensure secure access to information, in order to prevent unauthorized processing or processing without the necessary rights;

c) Ensure that the organization and third parties collaborate in the processing of information by adopting procedures aimed to complying with adequate levels of security;

d) Ensure that the organization and third parties that collaborate in the processing of information are fully aware of the security issues;

e) Ensure that anomalies and accidents affecting the information system and corporate security levels are promptly recognized and properly managed through efficient prevention, communication and reaction systems in order to minimize the impact on the business;

f) Ensure that access to offices and individual company premises is done exclusively by authorized personnel, to guarantee the safety of the areas and present assets;

g) Ensure compliance with legal requirements and compliance with the safety commitments established in contracts with third parties;

h) Guarantee the detection of anomalous events, accidents and vulnerabilities of information systems in order to respect the security and availability of services and information;

i) Ensure corporate business continuity and disaster recovery, through the application of established security procedures;

j) The information security policy is formalized in the ISMS, it is constantly updated to ensure its continuous improvement and it is shared within the organization, third parties and customers, through an intranet system and specific communication channels.

5 Information Security Policy Responsibility

The General Management is responsible for the secure information management system, in line with the evolution of the business and market context, by evaluating any actions to be taken in the face of events such as:

- significant business developments;
- new threats respect those ones considered in risk analysis activities;
- significant security incidents;
- evolution of the regulatory or legislative context regarding the secure processing of information.

All employees and all stakeholders are encouraged to play their part in achieving information security objectives.

Date: 21.07.2021

Quality Manager
Tatiana Bespalova