INTEGRATED MANAGEMENT SYSTEM POLICY

Aire Networks is a wholesale telecommunications operator with an operating license granted by the Spanish National Commission of Markets and Competition (CNMC), offering connectivity, voice, audiovisual, data hosting and security services to operators, companies and public bodies.

In the provision of professional telecommunications services, we are focused on the search for excellence at each and every process we undertake, with the aim of improving the experience and satisfaction of the client. Therefore, the decision was made to implement an Environmental Management System based on the ISO 9001 standard, in its current version.

In addition, aware of the current environmental impact, we consider respect for the environment as an integral value of our company in all the activities we perform and we, therefore, commit to carrying out environmental management in accordance with the current ISO 14001 standards, which helps to minimize harmful environmental impacts and promotes environmental protection and the prevention of pollution.

For the correct performance of our business functions and in order to ensure, when necessary, the access to an accurate, complete and confidential information, we developed an Information Security Management System based on the current ISO 27001 standards. This development is facilitated through the processing of different types of data and information and it is supported by systems, programs, communication infrastructures, files, databases, archives and so forth which make up part of the main assets that Aire Networks has so that the damage and loss of data/information affects the global performance of our services and it could jeopardize the continuity of the business.

In addition, through this Policy, Aire Networks establishes the framework for the development, establishment, review and improvement of the Business Continuity Plan (BCP) in accordance with the provisions of ISO 22301. This plan aims:

- To give an adequate and timely response to the materialization of both, safety and environmental risk of catastrophic features which causes a scenario of nonavailability of any of the basic components of the Grupo Aire activity: people, buildings and offices, technology, information and suppliers.
- To ensure that essential data and business functions are preserved during and after a catastrophe, minimizing disruption to daily operations. If data and business functions are not achieved during the disaster, they will be recovered gradually and in a timely manner until business normality is reached. The first goal is to reduce the impact of possible catastrophes on business activities.

Therefore, in order to guarantee the optimal quality of all services while respecting the environment, carrying out the appropriate information security measures and establishing the pertinent business continuity plans, there are three essential prerequisites: the management of quality, the environment and the information security. These requirements are considered essential to manage the following established principles:

- To obtain the **satisfaction** of clients, professionals and other stakeholders, committing to the

ISO 9001: 2015
Certificate 49446

ISO 14001: 2015
Certificate 62541

ISO / IEC 27001:2013
Certificate 64630

ongoing improvement of the services and a suitable attitude and aptitude with regard to the treatment of organizations to which services are provided in order to control and **reduce the number of incidents**, by means of a threefold approach: TRAINING, SERVICE and incident RESOLUTION.

- To fulfill all **legal and other requirements** to which Aire Networks adheres in relation to **the quality of the services** and the **impact associated with environmental aspects**.
- To maintain and continuously improve the efficiency of the management of Aire Networks, **increasing the quality** of the services provided and **minimizing pollution** by setting and reviewing **targets**, indicators, conducting audits, **improving environmental performance** and concluding in decision-making.
- To drive the **communication, training, awareness-raising and motivation** of professionals, collaborators and providers in matters related to quality and the environment.
- To improve internal processes taking into account the information security and the business continuity as well as the **prevention of pollution** and the **preservation of natural resources**, which could arise as a result of the activities and services carried out.
- To minimize the **environmental impact** of the activities carried out through the **efficient use of energy** and the **conservation of resources**, **waste reduction** and the prevention of pollution.
- By means of controls/measures, **protect the assets** against threats that could result in security incidents.
- **To curtail** the impacts of security **incidents**.
- **To establish** a system for **classifying information** and data with a view to protecting critical information assets.
- **To define responsibilities** with regard to information security and business continuity by creating the appropriate organization structure.
- **To prepare** a set of **rules, standards and procedures** applicable to the management bodies, employees, partners, external service providers, etc.
- **To specify** the effects of **non-compliance** with the Security Policy in the workplace.
- **To complete risk assessments of those critical process** which affects assets integrity in the event of a disaster with the aim of adopting both the appropriate security measures/control and the appropriate business continuity plans.
- **To verify** the correct operation of **security measures/controls and business continuity plans** by internal security audits carried out by independent auditors.
- **To Train users** in security management, information and communications technology, and business continuity.
- **To control the traffic of information and data** through communications infrastructures or the sending of optical, magnetic or paper data carriers etc.
- **To observe and comply with the law** in terms of data protection, intellectual property, labor law, information society services, criminal law, etc., which may affect Aire Networks' assets.
- **To protect the intellectual capital of the organization** so that it is not divulged or used illicitly.
- **To reduce** the possibility of **unavailability** through the adequate use of the organization's assets.

- **To defend the assets** against internal or external attacks so that they do not become security incidents.
- **To monitor the operation of the security measures**, investigating the number of incidents, their nature and impacts.
- **To protect all the staff** during a regular operation or an emergency situation.
- **To manage main risks** for the continuity of the processes considered critical by Aire Networks.
- **To minimize the impact** that could derive from any emergency situation in the processes, services or assets identified as critical.
- **To go back to the normal status** as soon as possible once the consequences of the incident have been mitigated.
- **Guarantee that both Continuity and Contingency plans** for disasters are developed and implemented properly by updating them when deemed necessary once periodic reviews are done and each time there is a significant change that may affect them in a continuous process improvement.

The whole Aire Networks team is responsible for complying with and enforcing this Integrated Management System Policy.

CEO

Elche, July 19, 2023