Aire Networks is a wholesale telecommunications services operator with a national operator's licence granted by the National Competition Market Commission in Spain that offers connectivity, voice, audiovisual, hosting and security services to operators, companies and public bodies.

For the correct performance of business functions and to be able to have access to information when necessary, to ensure that this information is complete and that its confidentiality is preserved, it was decided to implement an Information Security Management System based on the current **National Security Scheme (ENS)**. In this way, ENS controls and requirements are added for better compliance related to the services that can be offered to public administrations.

For this purpose, it is based on and assisted by the processing of different types of data and information, supported by systems, programmes, communications infrastructures, files, databases, archives, etc., which constitute one of Aire Networks' main assets, in such a way that their damage or loss affects the performance of its services and may jeopardise the continuity of the organisation.

In particular, for the provision of its OASIX business product services (Co-location and IaaS), Aire Networks is linked by electronic means, inter alia, with citizens, employees, customers and suppliers and other telecommunications service providers. These services must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, traceability, authenticity or confidentiality of the information processed or the services provided, in order to guarantee the quality of the information and the continuous provision of the services, acting preventively, supervising the daily activity and reacting promptly to any security incidents that may occur.

Thus, the Aire Networks systems required for the provision of these services must be protected against rapidly evolving threats with the potential to impact the confidentiality, integrity, traceability, authenticity, availability, intended use and value of information and services, and be prepared to prevent, detect, react and recover from incidents. To defend against these threats, a strategy is required to adapt to changing environmental conditions to ensure the continued provision of services. This implies that, without prejudice to the measures already adopted, both Aire Networks and its staff must apply the minimum security measures required by the **National Security Scheme (Royal Decree 311/2022, of 3 May, hereinafter also ENS),** as well as continuously monitor the levels of service provision, monitor and analyse reported vulnerabilities, and prepare an effective response to incidents that occur to ensure the continuity of the services provided.

For this reason, the different areas and departments of Aire Networks must be aware that security in information systems is an integral part of each stage of the life cycle of each of the Information Systems existing in Aire Networks, from their conception to their decommissioning, including the development or acquisition phases and the operating activities. It will also be taken into account that security requirements and the funding needs of these should be identified and included in the planning and tendering process.

Therefore, in order to guarantee optimum quality of all services, respecting the environment and with the appropriate information security measures (in compliance with the provisions of article 6, regarding integral security, and article 12, regarding security policy, of **Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme**), quality, environmental and information security management are considered essential requirements, establishing the following principles in their management:

1. Adoption and entry into force

Text approved by the Security Officer of the Information Security Management System (ISMS) of AIRE NETWORKS in session of 17/07/24. And which is ratified by the CEO of the company with the signature of this document.

This Information Security Policy shall be reviewed at least once a year to ensure that it is adapted to new technical or organisational circumstances that may arise.

This Policy is effective from the date of its approval until superseded by a new Policy.

2. Prevention, detection, reaction and response

Aire Networks Departments must be prepared to prevent, detect, react and recover from incidents, in accordance with Article 8 of the ENS.

2.1. Prevention

Departments should avoid, or at least prevent as far as possible, information or services from being compromised by security incidents. To this end, departments must implement the minimum security measures determined by the ENS, as well as any additional controls identified through a threat and risk assessment. These controls, and the security roles and responsibilities of all personnel, should be clearly defined and documented.

To ensure compliance with the policy, departments should:

- Authorise systems before going into operation.
- Regularly assess security, including assessments of configuration changes made on a routine basis.
- Request periodic review by third parties in order to obtain an independent assessment.

2.2. Detection

Since services can degrade rapidly due to incidents, ranging from a simple slowdown to a standstill, services must continuously monitor the operation to detect anomalies in service delivery levels and act accordingly.

Monitoring is particularly relevant when establishing lines of defence at different levels. Therefore, detection, analysis and reporting mechanisms will be put in place to reach those responsible on a regular basis and when there is a significant deviation from the parameters that have been pre-established as normal.

2.3. Response

Departments should:

- Establish mechanisms to respond effectively to security incidents.
- Designate point of contact for communications regarding incidents detected in other departments or other agencies.
- Establish protocols for the exchange of information related to the incident. This includes two-way communications with the Emergency Response Teams (CERTs).
- Contact the law enforcement authorities in accordance with the specific procedures provided for.
- Establish communication with emergency and civil protection bodies.
- **Mitigating** the effects of security **incidents** . For this purpose, Aire Networks bases its incident procedure on prevention, reaction and recovery.

2.4. Recovery

To ensure the availability of critical services, departments should develop systems continuity plans as part of their overall business continuity plan and recovery activities.

3. Outreach

3.1. Subjective scope:

This Policy applies to all Aire Networks staff members, and in particular to those who use, operate and administer the information and communications systems defined in the Scope of the Management System.

Accordingly, all Aire Networks personnel are obliged to be familiar with and comply with it.

It shall also apply, under the terms and conditions set out in section 12, to those third parties in which any of these circumstances apply:

(i) Third party organisations for whom Aire Networks provides services or from whom it handles information.

(ii) Third party service providers to Aire Networks or to whom information is provided.

3.2. Objective scope:

This Policy applies to all Aire Networks systems necessary for the provision of connectivity services, data centre hosting rental, fixed and mobile telephony, OASIX commercial product services (Co-location and IaaS) and the GECO transversal service related to the functions attributed to it by the legislation in force, and to the corporate mission stated in this Policy.

Specifically, it applies to the departments that support its value chain, the exercise of rights and the fulfilment of duties by electronic means, and the interaction by electronic means with customers, suppliers and other stakeholders covered by the MN-I-01 Integrated Manual.

4. Regulatory framework

Aire Networks, as a wholesale telecommunications operator, is governed by the provisions of Law 9/2014, of 9 May, General Telecommunications Law, in its sixteenth additional provision and the seventh, ninth and twelfth transitory provisions, and the General Telecommunications Law 11/2022.

In addition, and specifically insofar as they affect or may affect the subject matter of this Policy, the following are applicable to it:

- Royal Decree of 22 August 1885 publishing the Commercial Code.
- Royal Decree of 24 July 1889 publishing the Civil Code.
- Organic Law 10/1995 of 23 November 1995 on the Penal Code.
- Law 31/1995, of 8 November 1995, on the prevention of occupational hazards.
- Royal Legislative Decree 1/1996, of 12 April 1996, approving the revised text of the Intellectual Property Law, regularising, clarifying and harmonising the legal provisions in force on the matter.
- Law 34/2002 of 11 July 2002 on information society services and electronic commerce.
- Law 54/2003 of 12 December 2003 on the reform of the regulatory framework for the prevention of occupational risks.
- Royal Legislative Decree 1/2007, of 16 November, approving the revised text of the General Law for the Defence of Consumers and Users and other complementary laws.

- Law 3/2014, of 27 March, which amends the revised text of the General Law for the Defence of Consumers and Users and other complementary laws, approved by Royal Legislative Decree 1/2007, of 16 November.
- Law 21/2014, of 4 November, which amends the revised text of the Intellectual Property Law, approved by Royal Legislative Decree 1/1996, of 12 April, and Law 1/2000, of 7 January, on Civil Proceedings.
- Royal Legislative Decree 2/2015, of 23 October, approving the revised text of the Workers' Statute Law.
- Royal Decree 1720/2007, of 21 December, approving the Regulation implementing Organic Law 15/1999, of 13 December, on the protection of personal data.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights.
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Royal Decree-Law 14/2019, of 31 October, adopting urgent measures for reasons of public security in the areas of digital administration, public sector procurement and telecommunications.
- Royal Decree 311/2022 of 3 May, which regulates the National Security Scheme.
- Law 11/2022 of 28 June, General Telecommunications Law.

In any case, the foregoing shall be understood to be non-exhaustive and without prejudice to the provisions of any other applicable legislation.

5. Organisation of Information Security

The Management of Aire Networks, in the exercise of the ordinary management and administration functions of the entity and its services, is ultimately responsible for the promotion and compliance with the provisions of this policy and other Quality, Environment and Safety standards, guidelines and procedures that may be approved in the development of the same.

For the organisation, management and coordination of Quality, Environment and Information Security within Aire Networks, the following structure is in place with the functions and responsibilities detailed below:

- ISO Standards Committee
- CEO
- Security Officer
- Quality Manager
- Environment Officer
- Documentation Manager
- Information Officer
- Service Manager
- System Manager
- System Security Administrator

In the event of conflict between the different bodies entrusted with information security responsibilities, these shall be resolved by the functional superior and, ultimately, by the CEO.

In particular, the CEO of Aire Networks is competent to:

- The creation of the ISO Standards Committee
- The appointment of the Security Officer and his or her deputy.
- The appointment of Information Officers.
- The appointment of the Service Officers.
- The appointment of the System Manager.
- The appointment of System Security Administrators.

In other words, the Chief Information Officers, Service Officers, System Manager and Security Administrators will be appointed by the CEO, as Senior Management in the management system, either directly or through the ISO Standards Committee provided that the CEO is part of it.

The positions shall be renewed on an annual basis from the date of their appointment unless a new appointment is made by the competent bodies indicated in this section. In this case, the last appointment will be assumed as valid and the previously appointed positions will not be renewed, as they will cease to hold office in relation to the ENS and the integrated management system.

Finally, it is established that the meetings of the ISO Standards Committee will normally be attended by: the Security Officer, the Quality Manager, the Environment Manager and the Documentation Manager; in the event that technical information is required, the following will be summoned: the Information Managers, the Service Managers, the System Manager and the Security Administrators.

5.1. ISO STANDARDS COMMITTEE

5.1.1. COMMITTEE ESTABLISHMENT AND COMPOSITION:

An Information Security Committee has been set up under the name of "ISO Standards Committee", composed of the senior management representative and each of the responsible persons listed in this policy.

At the request of the Committee, any other person whose participation is deemed appropriate within the framework of the NSS may be invited to attend a meeting of the Committee.

Likewise, the Chairman of the ISO Information Standards Committee may agree to set up as many working groups as deemed necessary for the development of the functions entrusted to it.

5.1.2. RESPONSIBILITIES AND FUNCTIONS OF THE COMMITTEE:

The Information Security Committee coordinates information security within the management scope of the ISO Standards Committee, its main functions being the following:

- Establish and approve quality, environmental and information security objectives on an annual basis.
- Approve and review the Information Security Policy (ISO 27001, ISO 27018 and National Security Scheme).
- Review the documentation of the Integrated Management System.
- Assess the environmental aspects associated with the organisation's activity.
- Review the Annual Quality, Environment and Information Security Programme.
- Identify training needs and plan training actions.
- Review the final reports of the audits carried out.
- Check the follow-up and control of corrective actions and proposals for improvements.
- Approve environmental aspects as well as significant environmental aspects.
- Review and approve, in coordination with those responsible for the management systems, the changes that may affect them in order to guarantee sufficient resources and the correct management of the changes implemented.
- Approve the annual Internal Audit Plan and define the qualifications of internal auditors.
- Engage the auditors of a third party to carry out the external audit.
- Define and approve the indicators of the Integrated Management System.

- Resolve responsibility conflicts that may arise between different managers and/or different areas of the Organisation, escalating those cases where it does not have sufficient authority to decide.

5.1.3. FUNCTIONING OF THE COMMITTEE:

The Committee shall meet in ordinary session once a year and in extraordinary session when decided by its Chairman or when:

a) Serious security incidents occur that affect any area of Aire Networks' management scope.
b) New security needs arise that require the involvement of the Committee's components.

The Secretary of the ISO Standards Committee has the following functions:

- Convenes the meetings of the Information Security Committee.
- Prepares the topics to be discussed at Committee meetings, providing timely information for decision-making.
- It draws up the minutes of the meetings.
- It is responsible for the direct or delegated implementation of the Committee's decisions.

5.2. ROLES: ROLES AND RESPONSIBILITIES

5.2.1. CEO

The CEO's mission is based on demonstrating leadership and commitment to the Integrated Management System (Quality Management System, Environmental Management System, Information Security Management System and National Security Scheme).

Its functions and responsibilities are as follows:

- Assume responsibility and accountability for the effectiveness of the Integrated Management System.
- Ensure that the policy and objectives for quality, environment and information security (ISO 27001, ISO 27018 and National Security Scheme) are established and are compatible with the context and strategic direction of the organisation.
- Ensure the integration of the requirements of the Integrated Management System within the organisation's business processes.
- Promote the use of the process approach and risk-based thinking.
- Ensure the necessary resources for the Integrated Information Management System are available.
- Communicate the importance of effective quality, environmental and information security management in accordance with the requirements of the Integrated Management System.
- Ensure that the Integrated Management System achieves its intended results.
- Engage, lead and support people to contribute to the effectiveness of the Integrated Management System.
- Promote continuous improvement.
- Support other relevant management roles, to demonstrate leadership as it applies to their areas of responsibility.
- Determine, understand and regularly comply with customer and applicable legal and regulatory requirements.
- Identify and consider risks and opportunities that may affect the conformity of products and services and the ability to increase customer satisfaction.
- Maintain focus on increasing customer satisfaction.

5.2.2. SECURITY OFFICER

The Security Officer shall be responsible for the management of the Integrated Management System.

Its functions and responsibilities are as follows:

- Define, update and disseminate the IMS policy, procedures and formats.
- Propose the objectives of the IMS.
- Define the classification model and the management of the company's information assets.
- Assess the resources needed for Information Security.
- Perform and keep updated the information security risk analysis based on the provisions of the IMS.
- Define and implement the information security risk treatment plan.
- Propose and implement defined risk mitigation controls.
- Formulate risk management plans and monitor their implementation.
- Report results on measurable indicators.
- Propose improvements to the Information Security system.
- Plan and monitor the implementation of improvement measures or corrective actions and their effectiveness.
- Verify the implementation of the necessary security measures for the protection of SGI information.
- Promote information security training and awareness.
- Draw up a Statement of Applicability based on the security measures required under Annex II of the ENS and the outcome of the Risk Analysis.
- Provide the Information Controller and the Service Controller with information on the level of residual risk expected after implementing the processing options selected in the risk analysis and the security measures required by the ENS.
- Drawing up, together with the "Systems Manager", Safety Improvement Plans for approval by the ISO Standards Committee.
- Drawing up the Information Security Training and Awareness Plans for personnel, which must be approved by the ISO Standards Committee.
- Validate the Systems Continuity Plans prepared by the "Systems Officer", which shall be approved by the ISO Standards Committee and periodically tested by the Systems Officer.
- Approve the guidelines proposed by the CIO to consider Information Security throughout the lifecycle of assets and processes: specification, architecture, development, operation and changes.
- Evaluate and propose safeguards to prevent similar incidents in the future.
- Assess the risks of subcontracted activities.
- Evaluate suppliers in relation to Information Security.
- Conduct IMS security reviews.
- Ensure compliance with the Data Protection and Digital Rights Act and its European Regulation.

5.2.3. INFORMATION OFFICER

The Information Officer is the person who has the power to establish the information security requirements, i.e. to determine the levels of information security, having the ultimate responsibility for the use of certain information and, therefore, for its protection.

The Information Officer shall be the line manager of the department responsible for information management. When an information is covered by several Departments, the ISO Standards Committee may assume the status of Information Officer.

Its functions are:

- Classify information according to the criteria and categories established in the ENS and in each of the known and applicable security dimensions (availability, authenticity, traceability, confidentiality and integrity).
- The approval of the security levels shall be made at the proposal of the Information Security Officer or the System Manager.

- Validate the mandatory risk analyses and, together with the Service Managers and with the participation and advice of the Information Security Officer and the System Manager, select the safeguards to be implemented.
- Accept, together with the Service Officers, the residual risks calculated in the risk analysis, and monitor and control them, without prejudice to the possibility of delegating this task.

5.2.4. SERVICE MANAGER

The Service Manager is the person who has the power to establish the security requirements of the service, i.e. to determine the security levels of the services, having the ultimate responsibility for the use made of a given service and, therefore, for its protection.

The hierarchical superior of the department responsible for the provision of the service shall be the person in charge of the service. When a service depends on several Departments, the ISO Standards Committee may assume the status of Service Manager.

Its main functions are:

- Determine the security levels of the service in each of the known and applicable security dimensions (availability, authenticity, traceability, confidentiality and integrity).
- The approval of the security levels shall be made at the proposal of the Information Security Officer or the System Administrator.
- Validate the mandatory risk analyses and, together with the Information Officers and with the participation and advice of the Information Security Officer and the System Manager, select the safeguards to be implemented.
- Accept, together with the Chief Information Officers, the residual risks calculated in the risk analysis, and monitor and control them, without prejudice to the possibility of delegating this task.

5.2.5. SYSTEM MANAGER

The person responsible for:

- Develop, operate and maintain the System (understood as the set of information systems of Aire Networks) throughout its life cycle, from its specifications, installation and verification of its correct functioning.
- Define the topology and management policy of the System by establishing the criteria for its use and the services available in it.
- Ensure that specific security measures are properly integrated into the overall security framework.
- Agree to suspend the handling of certain Information or the provision of a certain Service if it is informed of serious security deficiencies that could affect the satisfaction of the established requirements. This decision must be agreed with the affected Information Officers, the affected Service and the Information Security Officer, before being executed
- Develop information security operating procedures.
- Collaborate with the Information Security Officer in the design of security improvement plans.
- Draw up the System Continuity Plan.
- Ensure compliance with the obligations of the System Security Administrator.
- Investigate security incidents affecting the system and report them to the Information Security Officer.
- Reporting to the Information Security Officer: (a) Security-related actions, in particular with regard to system architecture decisions. (b) Consolidated summary of security incidents. (c) The effectiveness of the protective measures to be put in place.
- Appointing System Officers Delegates. When, due to the complexity, distribution, physical separation or number of users of the information systems, additional personnel are required to carry out the functions of the System Officer, the System Manager may designate as many delegated System Officers as he/she

deems necessary. Such designation shall be approved in advance by the ISO Standards Committee, shall be made formally and shall entail the delegation of functions, but not of responsibility.

5.2.6. SYSTEM SECURITY ADMINISTRATOR

It is responsible for implementing, managing and maintaining the security measures applicable to the Information System.

Its main functions and responsibilities are:

- Manage, configure and update, where appropriate, the hardware and software on which the security mechanisms and services of the Information Systems are based.
- Implement, manage and maintain the security measures applied in the information systems.
- Supervise that security measures are strictly applied.
- Monitor the security status of the System.
- Manage the authorisations granted to users of the System, in particular the privileges granted, including monitoring that the activity carried out in the System is in accordance with what has been authorised.
- Implement Information Security Operating Procedures and Information Systems Operations.
- Monitor hardware and software installations, modifications and upgrades to ensure that security is not compromised and that they are at all times in compliance with the relevant authorisations.
- Report any security-related anomalies, compromises or vulnerabilities to the Information and System Security Officers.
- Collaborate in the investigation and resolution of security incidents, from detection to resolution.

5.2.1. QUALITY MANAGER

The Quality Manager is responsible for managing the Quality Management System (QMS) to ensure that services are appropriate, consistent and meet external and internal requirements.

Its main functions and responsibilities are:

- Maintain and manage all QMS documentation and records.
- Ensure that the quality management system functions correctly.
- Inform the rest of the organisation of changes or modifications to the QMS.
- Plan and establish quality procedures, standards and specifications.
- Ensure that all members of the organisation (internal and external) are aware of the quality objectives, understand them and respect them.
- Development of relevant QMS documentation.
- Implementing the implementation of the QMS in collaboration with the heads of the organisation's departments, controlling that the procedures, records and documentation approved by top management are applied.
- Carry out the measurement and monitoring of indicators, together with support staff as appropriate.
- Communicate the audit programme and follow up on the results of planned internal audits.
- Make suggestions for changes and improvements and how to implement them.
- Participate in the improvement of work processes.
- Review customer requirements and ensure that they are met.
- Establish, together with the Purchasing department, the quality requirements of external suppliers, verify that they follow the procedures and complete the documentation foreseen in the QMS.
- Follow up on procedures and non-conformities that may arise.
- Verify the effectiveness of corrective actions implemented for identified non-conformities.

5.2.2. ENVIRONMENTAL OFFICER

The Environmental Officer is responsible for managing the Environmental Management System (EMS).

Its main functions and responsibilities are:

- Prepare the relevant documentation according to the EMS.
- Maintain and manage all EMS documentation and records.
- Coordinate the development and control of all documents forming part of the EMS.
- Report to the top management of the organisation on the performance of the EMS.
- To implement the organisation's Environmental Policy.
- Define objectives, targets, deadlines, resources and actions according to the Environmental Policy.
- Analyse the degree of compliance with environmental objectives.
- Ensure that the EMS is implemented and properly maintained.
- Analyse the non-conformities detected in the different work areas.
- Establish corrective actions and proposals for improvement.
- Identify, together with the heads of departments, the environmental aspects associated with the organisation's activities.
- Ensure compliance with environmental legislation.
- Identify the environmental expectations of the organisation's customers.
- Determine what the environmental performance of suppliers will be.
- Implement, organise and manage environmental protection in the organisation.
- Organise training and awareness-raising plans for staff and their suppliers in relation to respect for the environment at work.
- Analyse the results of Internal and External Audits and file audit reports.
- Report to the ISO Standards Committee on the results of audits, both internal and external, and the corrective actions taken

5.2.3. DOCUMENTATION MANAGER

The Documentation Manager is responsible for managing the documentation that affects the Integrated Management System (IMS).

Its main functions and responsibilities are:

- Communicate the Policy to the staff of the organisation.
- Maintain up-to-date documentation control.
- Codification of the different procedures, records, protocols, manuals, etc., of the organisation.
- Communicate email configuration guidelines.
- Notify IMS to staff.
- Support the ISO Standards Committee in defining, disseminating and maintaining the Quality Management Policy and Principles.
- To safeguard and retrieve the documentation generated with the necessary efficiency so that it does not hinder the company's activity.
- Identify and control changes and current status of documents.
- Ensure that relevant versions of documents are available at points of use.
- Ensure that documents remain legible and easily identifiable.
- Prevent the unintended use of obsolete documents and apply appropriate identification to them in case they are kept for any reason.
- Organise documentation in a logical, efficient and categorised manner.

5.3. *APPOINTMENT AND RENEWAL PROCEDURES*

The Aire Networks Directorate is competent to:

- The creation of the Information Security Committee (ISO Standards Committee)

- The appointment of the Security Officer and his or her deputy.

- The appointment of Information Officers.

- The appointment of the Service Officers.

- The appointment of the Information Security Officer.

- The appointment of the System Manager.

- The appointment of System Security Administrators.

The Information Officers and Service Officers shall be appointed on the proposal of the ISO Standards Committee.

This competence shall be waived in the event that any of the above appointments have an impact on the organisation of the Entity.

The positions shall be renewed on an annual basis from the date of their appointment unless a new appointment is made by the competent bodies indicated in this section. In this case, the last appointment will be assumed as valid and the previously appointed positions will not be renewed, as they will cease to hold office in relation to the ENS and the integrated management system.

6. Personal data

In the performance of the functions attributed to it as a national telecommunications operator, it processes personal data and, in compliance with the applicable regulations, has a Security Document, which lists the files affected and the corresponding data controllers.

All Aire Networks information systems shall comply with the security measures based on the risk approach and other requirements regulated in REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter, RGPD) and Organic Law 3/2018 of 5 December 2018 on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD).

In addition, in order to improve regulatory support and provide greater transparency in compliance with personal data protection, the principles recommended by ISO 27018 should be followed, among others, some of which are listed below:

- There shall be a policy outlining guidelines for backups and requirements related to legal or contractual obligations related to the deletion of personal data contained in backups
- The retention period of administrative security policies and guidelines will be defined
- The creation of printed material or paper copies will be restricted
- Personal data restorations shall be monitored and recorded
- There shall be secure destruction of the paper medium, if processed by Aire Networks for the scopes defined
- ISO 27018 guidelines shall be taken into account for the preparation of contracts
- Suppliers will be managed through confidentiality clauses and subcontracting requirements
- There will be technical controls according to ISO 27018, some of them are listed: secure deletion of temporary files, event logging, protection of log information, control over data storage space pre-allocated to another client in the services offered under the OASIX environment.

7. Risk management

For all information systems within the scope of this Policy, a risk analysis shall be carried out, assessing the threats and risks to which they are exposed.

The risk analysis will be the basis for determining the security measures to be adopted in addition to the minimums established by the National Security Scheme, as provided for in Article 7 thereof.

This analysis will be repeated:

- Regularly, at least once a year.
- When the information handled changes.
- When the services provided change.
- When a serious security incident occurs.
- When serious vulnerabilities are reported.

For the harmonisation of risk analyses, the ISO Standards Committee will establish a baseline assessment for the different types of information handled and the different services provided.

The ISO Standards Committee will streamline the availability of resources to meet the security needs of the different systems by promoting horizontal investments.

8. Audit

While some of Aire Networks' information systems serve a basic category, there are others with a HIGH level categorisation. Consequently, it is considered appropriate to carry out an audit in accordance with Article 31 of the ENS, based on the following periods and criteria:

- **Ordinary:** Biennial period.
- **Extraordinary:** Whenever there are substantial modifications to the Information System, which may have an impact on the required security measures. The completion of the extraordinary audit shall determine the computation date for the calculation of the two years, established for the completion of the next regular ordinary audit, indicated in the previous paragraph.

9. Policy Development

This Policy will be further developed through more precise documents that will help to carry out what is proposed. For this purpose, the following will be used:

- Safety standards.

- Safety guides.

- Security procedures.

Security standards standardise the use of specific aspects of the system. They indicate the correct use and responsibilities of users. They are mandatory.

The guides have an educational character and aim to help users to correctly apply security measures by providing reasoning where precise procedures do not exist. For example, there is often guidance on how to write security procedures. The guides help to prevent overlooking important security issues that can materialise in a number of ways.

10. Awareness raising and training

In order to achieve full awareness that Information Security affects all Aire Networks staff members and all activities, in accordance with the principle of Integrated Security as stated in article 6 of the ENS, the ISO Standards Committee will establish an ongoing awareness programme for all Aire Networks staff members, in particular new recruits.

The ISO Standards Committee shall also develop and approve the necessary training requirements from an information security point of view.

11. Staff obligations

All members of Aire Networks are obliged to know and comply with this Policy and the Security Regulations, and it is the responsibility of the ISO Regulations Committee to provide the necessary means for the information to reach those affected.

12. Third parties

When Aire Networks provides services to other organisations or handles information from other organisations, they will be made aware of this Policy, channels will be established for reporting and coordination of the respective Information Security Committees and joint action procedures will be established for reacting to security incidents.

Where Aire Networks uses third party services or provides information to third parties, they will be made aware of this Policy and the Security Regulations that apply to those services or information. This third party shall be subject to the obligations set out in these rules and may develop its own operational procedures to satisfy them. Specific incident reporting and resolution procedures shall be established. It shall be ensured that third party personnel are adequately security-aware to at least the same level as set out in this Policy.

Where any aspect of this Policy cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Security Officer will be requested specifying the risks incurred and how they will be addressed. The approval of this report by those responsible for the information and services concerned shall be required prior to the use of or transfer of information to third party services.

13. Advertising and Communication

In order to ensure maximum dissemination of the Policy among Aire Networks' employees, it will be published on Aire Networks' internal resources.

Likewise, the security rules, guides and procedures approved in development of the ENS will be published in Aire Networks' internal resources. Exceptions may be made for documents which are classified as confidential due to their content.

All Aire Networks staff are responsible for complying with and enforcing this Information Security Policy

Raúl Aledo Coy

CEO

Elche, 24 September 2024