ENAIRE

Information Security Policy

Contents

1. INTRODUCTION 3
2. PURPOSE AND SCOPE 3
3. OPERATING PRINCIPLES AND COMMITMENTS 4
3.1. Purpose, Mission, and Vision 4
3.2. Commitments 5
3.2.1. Legal and Regulatory Framework 5
3.2.2. Information Security Objectives 5
3.2.3. Security Organisation 6
3.2.4. Information Security Committee 6
3.2.5. Roles and responsibilities 7
3.2.6. Legal Conformity 8
3.2.7. Structure of the Security Documentation 8
3.2.8. Risk Management 9
3.2.9. Audit and Business Continuity 9
3.2.10. Personal Data 9
3.2.11. Confidentiality of information 10
4. MONITORING MECHANISMS 10
5. DISCLOSURE AND DISSEMINATION 10
6. APPROVAL AND VALIDITY 11

1. INTRODUCTION

ENAIRE, a state-owned company of the Ministry of Transport, Mobility and the Urban Agenda, is responsible for, among other things, the planning, management, coordination, operation, maintenance and administration of air traffic, telecommunications and aeronautical information services, as well as of the communications infrastructure, facilities and networks of the air navigation system, with the aim of ensuring that the service is provided in a safe, efficient, continuous and sustainable manner.

After the publication of Royal Decree-Law 12/2018 of 7 September on the security of information networks and systems, implemented through Royal Decree 43/2021, dated 30 November 2018, ENAIRE was designated as Operator of Critical and Essential Services, thus highlighting the importance of the services it provides to its customers and to society as a whole.

ENAIRE, faithful to its safety, security, quality and efficiency principles, declares its firm commitment to achieving and maintaining the highest levels of cybersecurity, both in those operational systems directly involved in the provision of air navigation services, as well as in its corporate information systems, which are related to its business management and air navigation support services.

Through its different units, ENAIRE will promote and guarantee the continuous monitoring and supervision of all its technological infrastructure, the services provided and the informationhandled , ranging from office environments to the most critical operational settings.

To do this, on a technical level, effective mechanisms will be set up to prevent, detect, respond to and preserve the information and services of the organisation in the event of cybersecurity incidents through the corresponding technical units, both centrally and regionally.

The Cybersecurity Office, which directly reports to the Safety and Security Division, will coordinate corporate resources, develop and maintain the Information Security Management System (ISMS), enforce regulatory compliance and act as ENAIRE's intermediary and representative with relevant external bodies.

The Information Security Policy is consistent with the ISO/IEC 27000, 27001 and 27002 standards on Information Security Systems, the European and national regulations on personal data protection (GDPR and LOPDGDD), Royal Decree 311/2022 regulating the National Security Framework (NSF) and RD-Law 12/2018 on Network and Information Security, together with Royal Decree 43/2021 which implements it, structuring the efficient and effective management of cybersecurity in accordance with the standards and best practices of the sector.

2. PURPOSE AND SCOPE

This Information Security Policy aims to establish a baseline for ENAIRE's ISMS (Information Security Management System), and provide the operational framework for the organisation in terms of Information Security, taking into account the activities and services of the company, organisation, location, assets, technology, supply chain, the current and planned Information Security threat environment, the applicable laws, regulations and contracts, risk management strategy, as well as objective and target planning.

The goal of the ISMS, and thus of the Information Security Policy, is to protect information and services by guaranteeing its authenticity, confidentiality, integrity, availability, and traceability, as well as that of the information processing, transmission and storage assets.

This Information Security Policy shall be disseminated, known and applied to all internal and external personnel who have access to ENAIRE's information, and apply to all the activities, services, and technological resources that ENAIRE makes available to the organisation for the development of its own business. This Policy therefore affects the entire organisation, including the people who comprise the

Governing Board and the Steering Committee, and specifically, the information systems that support the services and processes that are necessary to implement and meet the business targets.

3. OPERATING PRINCIPLES AND COMMITMENTS

3.1. Purpose, Mission, and Vision

ENAIRE's **goal** in terms of cybersecurity is to reduce the risk and enhance the cyber resilience of its own services and operations in the sector, both at national and European level.

ENAIRE's **vision** in terms of cybersecurity is to be a highly cyber-resilient air navigation services provider, with a great capacity for resistance and recovery in response to a global panorama of constantly evolving threats.

ENAIRE's cybersecurity **mission** is to strengthen the efficiency, availability, safety and security of air navigation services in Spain and Europe through the deployment of cybersecurity capabilities, experience and knowledge, collaboration and information sharing with the different stakeholders in the sector, and continuous improvement in processes, technologies and awareness.

In order to achieve its Purpose, Mission, and Vision, ENAIRE establishes the following general principles for information security:

1. Security as a comprehensive process: Security is considered as a comprehensive process consisting of all the technical, human, material, strategic, legal, and organisational elements related to the system and its interconnections, aimed at guaranteeing prevention, detection, response, and preservation in the event of threats and incidents. ENAIRE's ISMS is part of the Integrated Management System (IMS) and is integrated into the organisation's processes (Government, Services and Support) and with the global management structure; therefore, information security is taken into account in the design of processes and systems throughout their life cycle.
2. Risk-based security management: ENAIRE's ISMS will ensure the confidentiality, integrity, availability, traceability, and authenticity of information and services by applying a continuous and permanently updated risk analysis and management process, while also considering the vendors and third parties involved.
3. Prevention, detection, response, and preservation: The management of security incidents considers security measures that implement prevention, detection, registration, classification, analysis, response, communication, and preservation mechanisms for any incident or significant deviation from parameters that are deemed normal. Additionally, business continuity will be part of the Management System, in accordance with the needs of the organisation, the established controls and the corresponding recovery and assurance plans of the most critical services.
4. Existence of a line of defence: ENAIRE's strategy for protecting its services relies on multiple layers of security, which consist of organisational, technological, physical, and logical measures, such that if any of them were to be compromised, the potential final impact would be minimal.
5. Continuous monitoring and periodic re-assessment: The organisation undertakes to continuously maintain and improve its ISMS through ongoing security monitoring processes and permanent assessments, in order to know the security status of systems and how to deal with deviations and exceptions (monitoring, audits, indicators, non-conformities, risk mitigation plans, etc.).

6. Allocation of responsibilities: ENAIRE organises its safety and security into specific organisational units and committees, engaging all the members of steering board. It designates different safety and security roles with separate responsibilities, coordination mechanisms and conflict resolution.
7. Resources: The organisation will determine and allocate the resources needed to establish, implement, maintain, and continuously improve the ISMS, including procurement and security services.
8. Evaluation of achievement of objectives: Strategic plans and information security objectives shall be set, and compliance with the results expected by the ISMS will be assessed.
9. Raising awareness and training: Training and awareness actions in Information Security will be implemented that are deemed necessary to ensure the competence of the organisation's employees in this area, regarding the specific needs of each job according to its duties.
10. Dissemination: The dissemination of best practices in terms of Information Security, as well as this Policy and the constant reinforcement of key messages, is critical in order to achieve a proper assimilation of fundamental principles that feed ENAIRE's know-how.

3.2. Commitments

3.2.1. Legal and Regulatory Framework

The definition of the Air Navigation System (ANS) and the services and systems that comprise it is laid out in Royal Decree 931/2010.

ENAIRE is subject to specific air navigation regulations, some of which cover aspects of information security. In particular:

- Commission Implementing Regulation (EU) 2017/373, laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight.
- Regulation (EU) 1029/2014, laying down requirements on the quality of aeronautical data and aeronautical information for the Single European Sky.
- Regulation (EC) 633/2007, laying down requirements for the application of a flight message transfer protocol used for the purpose of notification, coordination, and transfer of flights between air traffic control units.
- Royal Decree (RD) 311/2022 of 3 May, regulating the National Security Framework.

3.2.2. Information Security Objectives

Information Security objectives will be established for the relevant functions and levels, which will be:

- Consistent with this Information Security Policy.
- Measurable.
- Consistent with the results of the risk assessments.
- Documented, communicated, and updated, as per the procedure established for this purpose.

In general, this Policy sets out the following objectives:

- Comply with the applicable laws on the security of Information Systems.

- Ensure the confidentiality and integrity of data.
- Ensure the availability of Information Systems.
- Ensure the capacity to respond to emergency situations and restore critical services as soon as possible.
- Guarantee the authenticity of information in key processes.
- Maintain adequate traceability of the information in Information Systems when necessary.
- Promote ongoing training and awareness of Information Security.
- Enhance the implementation of best practices consistent with Royal Decree 311/2022 (Annex II), Royal Decree 12/2018 and ISO/IEC 27002.

3.2.3. Security Organisation

ENAIRE's Management provides the resources needed to guarantee the authenticity, confidentiality, integrity, availability, and traceability of the Information Systems for the normal conduct of employee activities and of the services provided to our customers. Management comprises the Cybersecurity and Security Committee, which will ensure compliance with the ISMS and the Information Security objectives. The document "Organisation of Information Security" describes in detail the structure, composition, operation, and specific tasks of the Information Security function in ENAIRE's organisation.

3.2.4. Information Security Committee

The Cybersecurity and Security Committee, called SECCIBE, will lead the organisation and promote a culture of Information Security, assigning the roles required and promoting the cross-cutting nature of cybersecurity in each process or service provided. The SECCIBE may be part of other Management Committees, but it will be responsible for coordinating, evaluating, and proposing improvements for Information Security and the services involved.

Similarly, there may be Information Security subcommittees, chaired by Information Security officers, which shall follow the guidelines established at general level. These management bodies materialise the principle of cooperation that must prevail in the Information Security structure at ENAIRE.

The SECCIBE will meet at least every quarter and its main functions include the following:

- Develop and coordinate the Information Security strategy and monitor its implementation.
- Advise the organisation on Information Security matters, resolving conflicts of responsibility in this area.
- Approve other policies, rules, and procedures related to Information Security.
- Promote the ongoing improvement of the ISMS in coordination with the head of the Integrated Management System. Participate in the review of the Management System.
- Receive status reports on security, cybersecurity, and safety and its impact on ENAIRE.
- Receive reports on the implementation status of regulations involving critical infrastructures at ENAIRE and adopt corrective measures.
- Control and monitor the actions and decision-making processes determined in previous committees, and analyse any possible deviations.
- Report to the Management Committee.

3.2.5. Roles and responsibilities

Information security mainly falls on three separate figures in the organisation. The Committee responsible for Information Security shall appoint and renew the members who hold the different roles and responsibilities, subject to approval by the Management Committee. These appointments will be reviewed every two years or when the position becomes vacant.

- Security Officer, part the Safety and Security Division, through the head of the Safety and Security Directorate. The main duties and responsibilities are:
    - Ensure the security of the information used and the services provided by the Information Systems.
    - Promote training and awareness campaigns on Information Security.
    - Manage the ISMS and coordinate with the other divisions, authorities, and external entities in the scope of Information Security.
    - Continuously conduct a risk analysis, assessing the impacts of cybersecurity incidents and updates and/or changes in systems and networks.
    - Manage and communicate to the competent authorities and bodies the different Information Security incidents that have occurred in the organisation, based on their level of criticality.
    - Prepare and keep updated the safety documentation within its scope of activity.
- Information Systems Officer, part of the Systems Division through the head of Systems Directorate. The main duties and responsibilities are:
    - Develop, operate, and maintain the Information Systems throughout the life cycle, their specifications, installation, and verify their correct operation.
    - Define the topologies and management systems of the Information Systems, establishing the criteria for use and the services provided by them.
    - Take the actions necessary to implement the Information Security measures resulting from the continuous improvement process and the ISMS Risk Management Plan corresponding to its areas.
- Information and Service Officers, part of the management units responsible for a particular service. The main duties and responsibilities are:
    - Establish requirements involving Information Security and the service they manage within their functional area of responsibility.
    - Define the different security levels, actively participating in the risk analysis and evaluating the assets under their responsibility in the security dimensions considered.
    - Collaborate in drafting the Information Security regulations within their scope of activity.

Also, ENAIRE, as a Critical Infrastructure and Essential Services Operator , has a Security and Liaison Officer, an Information Security Officer, and for each of these infrastructures, a Security Officer.

The Security and Liaison Officer will represent ENAIRE before State organisations in all matters relating to the security of its infrastructures and the different plans derived from it, channelling, where applicable, the operational and informative needs that arise in this regard.

The Information Security Officer will act as a point of contact with the competent authority in terms of overseeing the security requirements of information networks and systems, and as a specialised contact point with the relevant CSIRT.

Finally, each Security Officer will provide the operational link and the information channel with the competent authorities in all matters concerning the specific security of the critical infrastructure under their authority, channelling the operational and informative needs that relate to it.

Notwithstanding the above, all internal and external staff are responsible for the security and use of information within their functional and organic area of work, such that there is a joint responsibility between employees, managers, and the safety and security organisation. Failure to comply with this Policy and/or applicable internal regulations, both in terms of security and use of information and technological resources, may result in the application of any disciplinary measures deemed appropriate, in accordance with the established procedure, depending on the magnitude, impact and characteristics of the violation.

3.2.6. Legal Conformity

ENAIRE is firmly committed to ensuring compliance with the applicable laws and regulations on the protection and security of information, considering its purpose, corporate reason and business purpose. In this regard, the steering board has established as a security requirement that the legal and contractual obligations related to information and services be fully complied with. The requirements will be identified and organised for correct management in the document "Applicable Laws and Requirements".

Due to the nature and purpose of ENAIRE's business, there are laws, regulations, and legal provisions on, at least, aspects of air navigation services, the safety and security of critical infrastructures and essential services, intellectual property, protection of personal data, retention and storage of information that must be complied with and that will prevail, when applicable, over the guidelines contained in this Information Security Policy.

The rules issued by supranational bodies of which Spain is a member, and the Community and/or non-European Union regulations, will also be considered with regard to the services provided by ENAIRE.

3.2.7. Structure of the Security Documentation

This document lays out the high-level Information Security Policy. At a lower level, this Information Security Policy will rely on various mandatory policies, standards and procedures on specific topics that will be structured to meet the needs of certain groups within the organisation (use of technological resources, incident reporting, obligations, and duties, etc.). The development, classification and processing of the security documentation will follow the guidelines of ENAIRE's Document Management process.

In addition, the goals that ENAIRE aims to achieve with the application of its ISMS shall be defined and evaluated to determine the effectiveness of the ISMS.

As part of the ISMS, different specific procedures shall be developed that will include the technical details necessary for the application of the security controls.

All these documents will be accessible to all employees of the organisation, both internal and external, insofar as they are necessary based on their "need to know" for the proper performance of their duties in the company. In this regard, all ENAIRE members are required to know and comply with this Information Security Policy and Security Regulations.

3.2.8. Risk Management

ENAIRE will apply an Information Security risk management process that:

- Lays out and maintains criteria on Information Security risks, including:
  - The risk acceptance criteria.
  - The criteria for conducting risk assessments.
- Ensures that successive risk assessments create consistent, valid, and comparable results.
- Identifies the threats to Information security.
- Analyses the threats to Information Security by:
  - Assessing the possible consequences that would result if the threats identified were to materialise.
  - Realistically assessing the likelihood of the threats identified.
  - Determining risk levels.
- Evaluates Information Security risks by:
  - Comparing the results of the risk analysis with the established risk criteria.
  - Prioritising the processing of the risks analysed.
- Processes the risks to Information Security to:
  - Select the appropriate risk mitigation options taking into account the results of the risk assessment.
  - Determine the necessary safeguards to implement the chosen risk mitigations.
  - Prepare an Information Security Risk Mitigation Plan.

Risk management processes will be carried out periodically at planned intervals, or when significant changes are proposed or made. Documentary records will be kept of all risk management processes.

3.2.9. Audit and Business Continuity

The Information Systems, in whole or in part, will be subject to periodic internal and external audits to verify their proper operation, determining levels of compliance and recommending corrective measures for continuous improvement.

The administration of service continuity is a critical process that must consider involving the entire organisation. The development and implementation of Continuity Plans will ensure that essential services can be restored within the required deadlines, including controls aimed at identifying and reducing risks, and that the possible consequences of potential service interruptions can be mitigated. These Plans shall be regularly tested, reviewed, and updated to ensure their continued effectiveness.

3.2.10. Personal Data

ENAIRE processes personal data, for which it has a Personal Data Processing Manual in accordance with Regulation (EU) 2016/679. This Protocol, including the risk analysis of personal data processing, includes all the initial elements required to comply with the data protection regulation, defining and establishing essential aspects to ensure the due diligence of the responsible party.

For all purposes, this policy complies with (EU) Regulation 2016/679 of the European Parliament and Council of 27 April 2016 concerning the protection of individuals regarding the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). It likewise complies with Organic Law 3/2018 of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights.

All of ENAIRE's information systems shall conform to the security levels required by law for the nature and purpose of the personal data set out in the aforementioned Security Protocol. Similarly, it shall adopt the technical and organisational measures necessary to comply with the data protection regulations in force in each case. The Central Data Protection Unit is available to provide specific support and advice in this regard.

3.2.11. Confidentiality of information

Both internal and third-party employees (e.g., technical assistance or external services) who work for or on behalf of ENAIRE shall preserve and protect the information, data, services, and assets of ENAIRE, using them strictly to carry out their duties, and committing not to disclose or publish information, data, images or content of any nature or format (digital or physical) that is the property of ENAIRE or related to ENAIRE, its employees, resources, systems, operations, facilities or infrastructures, which they were able to access or know about thanks to their relationship with ENAIRE, without an explicit and formal authorisation, as per the internal rule on the Use of Technological Resources.

ENAIRE will ensure compliance with these principles, applying the appropriate restrictions and, where applicable, the disciplinary regime.

4. MONITORING MECHANISMS

Steering board has established the strategic lines to ensure that these commitments materialise into actions and results, and undertakes to make available the resources needed to provide our services while managing economic resources with efficiency criteria.

Given the relevance of the questions related to Information Security, specific functions are attributed to specialised committees, such as the Cybersecurity and Security Committee of ENAIRE.

The Steering Committee will oversee the promotion and implementation of this Policy, and, through the CEO, inform the Governing Board of its progress, where relevant, in accordance with the processes established for its review as part of the Integrated Management System.

5. DISCLOSURE AND DISSEMINATION

This Policy is supported by Senior Management and is kept as substantiated information.

When ENAIRE provides services to other bodies or uses third-party services, it will engage with them on this Information Security Policy and the security regulations related to such services, and establish coordination and reporting channels.

In compliance with the requirements of international transparency standards and practices, this Policy will be made available to all stakeholders on ENAIRE's website for their information and consultation.

Similarly, it will be suitably communicated and disseminated internally using existing tools to ensure it is understood and applied within the organisation, thus confirming ENAIRE's commitment to our staff, to development and progress in order to guarantee the future of aviation and Spanish society, promoting its dissemination so it is understood by all the people who act on behalf of ENAIRE.

6. APPROVAL AND VALIDITY

Following its presentation to the Steering Committee on 19 April 2023, this Policy was approved by ENAIRE's Governing Board at its meeting of 26 April 2023, coming into force on that date. It shall remain in force until amendments are made to the Policy, which will be properly communicated.

This Policy is subject to review and updating as needed to adapt it to any regulatory, social, economic, or organisational changes.