



Information Security Policy

Contents

1. INTRODUCTION	3
2. PURPOSE AND SCOPE.....	3
3. 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	6
3.2.3. Security Organisation	6
3.2.4. Information Security Committee	6
3.2.5. Roles and Responsibilities	7
3.2.6. Legal Compliance	9
3.2.7. Security Documentation Structure	9
3.2.8. Risk Management.....	9
3.2.9. Security Event Management	10
3.2.10. Supply Chain	10
3.2.11. Audit and Business Continuity	10
3.2.12. Personal Data	11
3.2.13. Confidentiality of Information	11
4. OVERSIGHT MECHANISMS	11
5. PUBLICATION AND DISSEMINATION	12
6. APPROVAL AND ENTRY INTO FORCE	12

1. INTRODUCTION

ENAIRe, a public business entity attached to the [Ministry of Transport and Sustainable Mobility](#), is responsible, among other duties, for planning, directing, coordinating, operating, maintaining and administering air traffic, telecommunications and aeronautical information services, together with the infrastructure, facilities and communications networks of the air navigation system, with the aim of ensuring that services are provided safely, efficiently, continuously and sustainably.

Following the publication of Royal Decree-Law 12/2018 on the security of network and information systems, subsequently developed by Royal Decree 43/2021, ENAIRe was designated a [Critical Operator and Essential Services Operator](#) on 30 November 2018, reflecting the importance of the services it provides to its customers and to society as a whole.

In keeping with its principles of safety, quality and efficiency, ENAIRe declares its firm commitment to achieving and maintaining the highest levels of cybersecurity in both the [operational systems](#) directly involved in the provision of air navigation services and the [corporate information systems](#) that support business management and air navigation.

Through its various units, ENAIRe will promote and ensure the [continuous supervision and monitoring](#) of all its technological infrastructure, services and information, ranging from office IT environments to its most critical operational environments.

To this end, effective technical mechanisms will be put in place to [prevent, detect and respond](#) to cybersecurity incidents and to maintain the organisation's information and services, through the relevant technical units at both central and regional level.

The [Cybersecurity Office](#), which reports to the Security Division, will coordinate corporate resources, develop and maintain the Information Security Management System (ISMS), oversee proper regulatory compliance and act as ENAIRe's point of contact and representative before the relevant external bodies.

The [Information Security Policy](#) is aligned with the international ISO/IEC 27000 family of Information Security standards; European and national personal data protection legislation, including the GDPR and LOPDGDD; Royal Decree 311/2022 regulating the National Security Framework (ENS); and the NIS2 Directive on the security of network and information systems. It provides a structure for managing security efficiently and effectively in accordance with these requirements and with industry best practice.

It also takes account of Regulation (EU) 2017/373 laying down common requirements for providers of air traffic management and air navigation services and other air traffic management network functions and their oversight, together with Regulation (EU) 2023/203 (PART-IS), laying down rules for the application of Regulation (EU) 2018/1139 as regards requirements for managing information security risks with a potential impact on aviation safety. In relation to the latter, ENAIRe undertakes to comply with its provisions and with the [Information Security Management Manual \(ISMM\)](#) prepared for this purpose.

2. PURPOSE AND SCOPE

This [Information Security Policy](#) provides the foundation for ENAIRe's Information Security Management System (ISMS) and sets out the framework governing the organisation's approach to Information Security. It takes account of ENAIRe's activities and services, organisational structure, locations, assets, technology and supply chain; the current and anticipated Information Security threat environment; applicable legislation, regulations and contracts; its risk management strategy; and the planning of objectives and targets.

The purpose of the ISMS, and therefore of this Policy, is to protect information and services by ensuring their **authenticity, confidentiality, integrity, availability and traceability**, together with that of the assets used to process, transmit and store information.

This Information Security Policy will be **communicated to, understood and applied** by all internal and external personnel with access to ENAIRE information, and will apply to all activities, services and technological resources made available by ENAIRE for the conduct of its business. Accordingly, this Policy applies throughout the organisation, including to members of the Governing Board and Management Committee, and specifically to the information systems that support the services and processes required to achieve ENAIRE's business objectives.

3. PRINCIPLES AND COMMITMENTS

3.1. Purpose, Mission and Vision

ENAIRE's **purpose** in cybersecurity is **to reduce risk and increase** cyber resilience across both its own services and operations and the wider sector in Spain and Europe.

ENAIRE's cybersecurity **vision** is to become a **highly cyber-resilient** air navigation services organisation, with a strong ability to withstand and recover from an ever-evolving global threat landscape.

The **mission** of cybersecurity at ENAIRE is **to strengthen the efficiency, availability and security of air navigation services** in Spain and Europe by deploying cybersecurity capabilities, drawing on expertise and knowledge, collaborating and sharing information with sector stakeholders, and continuously improving processes, technologies and awareness.

To achieve its **Purpose, Mission and Vision**, ENAIRE establishes the following general Information Security principles:

1. **Security as an end-to-end process:** Security is understood as an end-to-end process, secure by default and by design, encompassing all technical, human, material, strategic, legal and organisational elements relating to the system and its interconnections and aimed at ensuring the prevention, detection, response and preservation required to address threats and incidents. ENAIRE's ISMS will form part of the Integrated Management System (IMS) and will be embedded in the organisation's Governance, Services and Support processes and its overall management structure. Information Security will therefore be taken into account when designing processes and systems throughout their life cycle.
2. **Risk-based security management:** ENAIRE's ISMS will preserve the confidentiality, integrity, availability, traceability and authenticity of information and services through a continuous and regularly updated risk analysis and management process that also covers the suppliers and third parties involved.
3. **Prevention, detection, response and preservation:** Security incident management includes measures that provide mechanisms for preventing, detecting, recording, classifying, analysing, responding to, communicating and preservation of information concerning any incident or significant deviation from the parameters established as normal. Business continuity will also form part of the Management System, in line with the organisation's needs, the controls in place and the corresponding recovery and service assurance plans for the most critical services.
4. **Defence in depth:** ENAIRE's service protection strategy is based on multiple layers of security comprising organisational, technological, physical and logical measures, so that if one layer is compromised, the resulting impact is kept to a minimum.

5. **Continuous monitoring and periodic reassessment:** The organisation is committed to continuously maintaining and improving its ISMS through ongoing monitoring and regular security assessments, in order to understand the security status of its systems and manage deviations and exceptions through monitoring, audits, indicators, non-conformities and risk treatment plans, among other measures.
6. **Clear separation of responsibilities:** ENAIRe organises its security function through dedicated organisational units and committees, involving all members of company management. It assigns distinct security roles with clearly differentiated responsibilities, together with coordination and conflict-resolution mechanisms.
7. **Resources:** The organisation will determine and allocate the resources needed to establish, implement, maintain and continually improve the ISMS, including the procurement of security products and services.
8. **Monitoring achievement of objectives:** Information Security strategic plans and objectives will be established, and achievement of the results expected from the ISMS will be assessed.
9. **Training and awareness:** Information Security training and awareness initiatives will be implemented as necessary to ensure that the organisation's personnel have the required competence in this area, taking account of the specific needs of each profile and role.
10. **Communication and dissemination:** Communicating good Information Security practices and this Policy, and continuously reinforcing its core messages, are critical to embedding fundamental principles and strengthening ENAIRe's knowledge base.

3.2. Commitments

3.2.1. Legal and Regulatory Framework

ENAIRe is subject to a range of regulations, some of which address Information Security matters. Given their particular relevance, the following are listed by way of illustration:

- Commission [Implementing Regulation \(EU\) 2017/373](#) of 1 March 2017 laying down common requirements for providers of air traffic management and air navigation services and other air traffic management network functions and their oversight.
- [Royal Decree 311/2022](#) of 3 May regulating the National Security Framework ([ENS](#)).
- Commission [Implementing Regulation \(EU\) 2023/203](#) of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council as regards requirements for managing information security risks with a potential impact on aviation safety ([PART-IS](#)).
- Commission [Regulation \(EU\) 2015/340](#) of 20 February 2015 laying down technical requirements and administrative procedures relating to air traffic controllers' licences and certificates.
- [Commission Implementing Regulation \(EU\) 2021/664](#) of 22 April 2021 on a regulatory framework for the [U-space](#).
- Commission [Delegated Regulation \(EU\) 2022/1645](#) of 14 July 2022 on requirements for managing information security risks with a potential impact on aviation safety in the context of Apron Management Services ([AMS](#)).
- Commission [Implementing Regulation \(EU\) 2023/1769](#) of 12 September 2023 on the design or production of air traffic management and air navigation services systems and constituents ([DPO](#)).

- [Directive \(EU\) 2022/2555](#) of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union ([NIS2](#)).
- [Directive \(EU\) 2022/2557](#) of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities ([CER](#)).

3.2.2. Information Security Objectives

Information Security objectives will be established at the relevant functions and levels and will be:

- [Consistent](#) with this Information Security Policy.
- [Measurable](#).
- [Consistent](#) with the results of risk assessments.
- [Documented](#), [communicated](#) and [updated](#) in accordance with the procedure established for this purpose.

As a general principle, this Policy sets out ENAIRe's approach to the impact that Information Security risks may have on operational safety. The following objectives are therefore established within the ISMS:

- [Comply](#) with applicable legislation on information systems security and take account of relevant standards and best practices in this area.
- Ensure [data confidentiality](#) and [integrity](#).
- Ensure the [availability](#) of information systems.
- Ensure the [ability](#) to respond to emergencies by restoring critical services as quickly as possible.
- Ensure the [authenticity](#) of information in key processes.
- Maintain adequate [traceability](#) of information within information systems where required.
- Promote continuous Information Security [training](#) and [awareness](#).
- Promote the implementation of [good practices](#) aligned with Royal Decree 311/2022 (Annex II), the NIS2 Directive and ISO/IEC 27002.

To achieve these objectives, ENAIRe uses a set of measures and performance indicators included in its Cybersecurity Dashboards and reviewed by the various committees responsible for Information Security. These allow the organisation to continuously monitor compliance with the objectives established.

3.2.3. Security Organisation

ENAIRe's Management assumes responsibility for Information Security as one of its core duties and therefore ensures that the [resources](#) needed to protect the authenticity, confidentiality, integrity, availability and traceability of information systems are available, so that ENAIRe personnel can carry out their activities normally and services can be provided to customers. Management has established the [Cybersecurity and Physical Security Committee](#), known as SECCIBE, which oversees compliance with the ISMS and the Information Security objectives.

ENAIRe has specific documents that set out in detail the structure, membership, operation and specific tasks of the Information Security function within the organisation.

3.2.4. Information Security Committee

SECCIBE will [lead ENAIRe's Information Security organisation and promote a culture of Information Security](#) by assigning the required roles and embedding security across every process and service provided. SECCIBE may participate in other management committees, but will remain responsible for

coordinating and assessing Information Security and the services concerned and for proposing improvements.

Information Security subcommittees may also be established, chaired by the designated Information Security Delegates, and must follow the guidelines established at organisation-wide level. These management bodies put into practice the principle of cooperation that must underpin ENAIRe's Information Security organisation.

SECCIBE will meet at least quarterly. Its [main functions](#) include:

- [Develop and coordinate](#) the Information Security strategy and monitor its implementation.
- [Advise](#) the organisation on Information Security matters and resolve conflicts over responsibilities in this area.
- [Approve](#) other Information Security policies, standards and procedures.
- [Promote](#) the continuous improvement of the ISMS in coordination with the person responsible for the Integrated Management System. Participate in the review of the Management System.
- Receive [reports on the status of physical, logical and operational security](#) and its impact on ENAIRe.
- Receive [reports on the implementation status of critical infrastructure regulations](#) at ENAIRe and adopt corrective measures.
- Monitor [and follow up](#) the actions and decisions agreed at previous committee meetings and analyse any deviations.
- [Report](#) to the Management Committee.

3.2.5. Roles and Responsibilities

The principal organisational role within the Information Security framework is that of the [Accountable Manager](#), held by ENAIRe's Director General as the person with ultimate responsibility for the organisation. The main duties and responsibilities are:

- Sign this Policy and oversee compliance with it, ensuring that all personnel in the organisation are aware of it.
- Ensure that the organisation has the resources required to meet its Information Security needs.
- Ensure that all personnel in the organisation understand their Information Security responsibilities.
- Ensure that all personnel in the organisation receive the necessary Information Security training.

The Information Security structure below this level is based primarily on three distinct organisational roles. The committee responsible for Information Security will appoint and renew the individuals assigned to the various roles and responsibilities, subject to ratification by the Management Committee. These appointments will be reviewed every two years or whenever a position becomes vacant.

- [The Security Manager role](#) sits within the Security Division and is held by the Head of the Security Division. The main duties and responsibilities are:
 - Maintain the security of information handled by, and services delivered through, the Information Systems.
 - Promote Information Security training and awareness campaigns.
 - Administer the ISMS and coordinate Information Security matters with the other divisions, authorities and external bodies.

- Carry out ongoing Risk Analysis, assessing the impact of security incidents and of updates and/or changes to systems and networks.
- Manage Information Security incidents within the organisation and report them to the competent authorities and bodies according to their severity.
- Prepare and keep up to date the security documentation within their area of responsibility.
- **The Systems Manager role** sits within the Systems Directorate and is held by the Systems Director. The main duties and responsibilities are:
 - Develop, operate and maintain the Information Systems throughout their life cycle, including their specifications, installation and verification of correct operation.
 - Define Information System topologies and management systems, setting their conditions of use and available services.
 - Implement the actions required to apply the Information Security measures arising from the continuous improvement process and the ISMS Risk Treatment Plan that fall within their areas of responsibility.
- **The Information and Service Owner** roles sit within the Directorates responsible for individual services, under the leadership of the Directorate General. The main duties and responsibilities are:
 - Set the Information Security and service requirements for the services they manage within their functional areas of responsibility.
 - Define the various security levels, participate actively in the Risk Analysis and assess the assets for which they are responsible against the relevant security dimensions.
 - Help draw up the Information Security rules within their area of responsibility.

The **Compliance Monitoring Manager under Regulation (EU) 2023/203** is the same person appointed under Regulation (EU) 2017/373, namely the Head of the Internal Audit Division. The Compliance Monitoring Manager's membership of SECCIBE ensures appropriate communication and coordination with the other Information Security roles, including the ISMS Manager and the *Accountable Manager*, and with the other committee members, in accordance with their respective responsibilities.

ENAIRe, as a Critical Infrastructure Operator and Essential Entity, also has a Security and Liaison / Resilience Officer, a Chief Information Security Officer and, for each such infrastructure, an appointed Security Delegate.

The **Security and Liaison / Resilience Officer** will represent ENAIRe before State bodies in all matters relating to the security of its infrastructure and the associated plans, channelling any operational and information requirements that arise.

The Chief **Information Security Officer (CISO)** will act as the point of contact with the authority responsible for overseeing network and information system security requirements and as the specialist point of contact with the relevant *Computer Security Incident Response Team (CSIRT)*.

Each **Security Delegate** will act as the operational liaison and information channel with the competent authorities on all matters relating to the security of the critical infrastructure for which they are responsible, channelling the related operational and information requirements.

The **Data Protection Officer (DPO)** will ensure compliance with the applicable legislation in this area through the corporate Central Data Protection Unit (UCPD). The DPO will also act as the Point of Contact (POC), where required, in relation to personal data processing.

Notwithstanding the above, all internal and external personnel working for ENAIRE are responsible for the security and use of information within their functional and organisational remit. [Responsibility is therefore shared by all personnel, including managers and the security organisation](#). Failure to comply with this Policy and/or the applicable internal rules governing security, the use of information or technological resources may result in appropriate disciplinary action under the established procedure, depending on the scale, impact and nature of the breach.

3.2.6. Legal Compliance

ENAIRe is [firmly committed to](#) ensuring compliance with current legislation and regulations on information protection and Information Security, taking account of its purpose, corporate name and business objectives. Management has therefore established full compliance with legal and contractual obligations relating to information and services as a security requirement. The requirements will be identified and organised for proper management in the 'Applicable Legislation and Requirements' document.

Given the nature and purpose of ENAIRE's business, it must comply with legislation, standards and legal provisions governing at least air navigation services; the security of Critical Infrastructure and Essential Entities; intellectual property; personal data protection; and information retention and storage. Where applicable, these requirements will take precedence over the guidelines set out in this Information Security Policy.

Standards issued by supranational bodies of which Spain is a member, together with EU and/or non-EU legislation, will also be taken into account in light of the areas in which ENAIRE provides services.

3.2.7. Security Documentation Structure

This document sets out the high-level Information Security Policy, alongside other top-level corporate policies in different areas.

At the next level, this Information Security Policy will be supported by mandatory policies, standards and procedures on specific matters, structured to meet the needs of particular groups within the organisation (use of technological resources, incident reporting, obligations and duties, etc.). The development, classification and handling of security documentation will follow [ENAIRe's Document Management](#) process.

The objectives that ENAIRE seeks to achieve through its Information Security Management System will also be defined and evaluated to determine the effectiveness of the ISMS.

As part of the ISMS, specific procedures will be developed in sufficient technical detail to apply the security controls.

All these documents will be [available](#) to internal and external personnel as required on a 'need-to-know' basis for the proper performance of their duties at ENAIRE. Accordingly, all ENAIRE personnel must be familiar with and comply with this Information Security Policy and the applicable security rules.

3.2.8. Risk Management

ENAIRe will apply an [Information Security risk management process](#) that:

- [Establishes and maintains](#) Information Security risk criteria, including:
 - Risk acceptance criteria.
 - Criteria for carrying out risk assessments.
- [Ensures](#) that successive risk assessments produce consistent, valid and comparable results.
- [Identifies](#) Information Security threats.

- **Analyses** Information Security threats by:
 - Assessing the potential consequences if the identified threats were to materialise.
 - Realistically assessing the likelihood of the identified threats occurring.
 - Determining risk levels.
- **Evaluates** Information Security risks by:
 - Comparing the results of the Risk Analysis with the established risk criteria.
 - Prioritising the treatment of the risks analysed.
- **Treats Information Security risks** by:
 - Selecting appropriate risk treatment options in light of the risk assessment results.
 - Determining the safeguards required to implement the chosen risk treatment.
 - Drawing up an Information Security Risk Treatment Plan.

Risk management processes will be carried out periodically at planned intervals and whenever significant changes are proposed or made. Documentary records of all risk management processes will be retained.

3.2.9. Security Event Management

ENAIRe will have a procedure for the prompt management of security events (incidents or vulnerabilities) that pose a threat to information and services, within the ISMS and in compliance with all applicable Information Security legislation and regulations.

The organisation will therefore encourage personnel to report any vulnerabilities, suspicious or anomalous events and/or Information Security incidents detected in day-to-day operations. The purpose is to learn from them and improve Information Security, while ensuring the confidentiality and protection of those who report them, in accordance with ENAIRe's Just Culture Policy.

ENAIRe will also coordinate internal and external communications concerning such events and, where appropriate, notify the relevant CSIRT and any other body or entity requiring notification.

3.2.10. Supply Chain

ENAIRe establishes the criteria and controls needed to ensure that service providers, third parties and processors with access to the organisation's information, systems or services comply with the security requirements of the National Security Framework (ENS) and all other applicable legislation and regulations.

To this end, suppliers are classified according to their security impact; security requirements appropriate to the level of service provided are established and formalised in contractual agreements; and compliance is monitored periodically. Supplier access to information assets and services is also strictly controlled, security incidents are properly managed, and measures are in place to revoke access and protect information when the contractual relationship ends. A POC (Point or Person of Contact) is designated for Information Security matters.

3.2.11. Audit and Business Continuity

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

Service continuity management is a critical process that should involve the entire organisation. The development and implementation of Business Continuity Plans will ensure that essential services can be

restored within the required timeframes. The plans will include controls to identify and reduce risks and mitigate the potential consequences of service interruptions. These plans must be tested, reviewed and updated periodically to ensure their continued effectiveness.

3.2.12. Personal Data

ENAIRe [processes personal data](#) and has a Personal Data Processing Manual in accordance with 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, repealing Directive 95/46/EC, known as the General Data Protection Regulation (GDPR). This Manual, including the risk analysis for personal data processing, contains all the initial elements required to comply with data protection legislation and defines the key aspects needed to enable the controller to exercise due diligence.

For all purposes, this Policy complies with the General Data Protection Regulation (GDPR). It also complies with Organic Law 3/2018 of 5 December on Personal Data Protection and Guarantee of Digital Rights (LOPDGDD).

All ENAIRe information systems will meet the security levels required by law for the nature and purpose of the personal data covered by the aforementioned Security Protocol. ENAIRe will also adopt the technical and organisational measures required to comply with the data protection legislation applicable in each case. The Central Data Protection Unit (UCPD), led by the Data Protection Officer (DPO), acts as the centre for specialist support and advice in this area.

3.2.13. Confidentiality of Information

All ENAIRe personnel and third-party personnel (e.g. technical support staff or external service providers) working for or on behalf of ENAIRe must [safeguard and protect](#) ENAIRe's information, data, services and assets and use them strictly in the performance of their duties. They undertake not to disclose, without express formal authorisation and in accordance with the internal rules on the [Use of Technological Resources](#), any information, data, images or content of any nature or format (digital or physical) owned by or relating to ENAIRe, its employees, resources, systems, operations, facilities or infrastructure, to which they have gained access or of which they have become aware through their relationship with ENAIRe.

ENAIRe will ensure compliance with these principles by applying the appropriate restrictions and, where applicable, disciplinary procedures.

4. OVERSIGHT MECHANISMS

Management has established the strategic guidelines required to translate these commitments into action and results and undertakes to provide the resources needed to deliver our services, while managing financial resources efficiently.

Given the importance of Information Security matters, specific functions are assigned to specialist committees such as ENAIRe's Cybersecurity and Physical Security Committee.

The [Management Committee](#) will oversee the promotion and rollout of this Policy. Through the Director General, it will report progress to the [Governing Board](#) where appropriate, in accordance with the processes established for its review within the Integrated Management System.

5. PUBLICATION AND DISSEMINATION

This Policy is endorsed by Senior Management and maintained as documented information.

When ENAIRE provides services to other [bodies](#) or uses [third-party services](#), those bodies or providers will be made aware of this Information Security Policy and the security rules relating to those services, and coordination and reporting channels will be established.

In accordance with international standards and transparency practices, this Policy will be available to all stakeholders on ENAIRE's [website](#) for information and consultation.

It will also be communicated internally through the available tools to ensure that it is understood and applied throughout the organisation. This will reaffirm ENAIRE's [commitment](#) to its people and to the development and [progress](#) needed to secure the future of the aviation sector and Spanish society, while ensuring that the Policy is understood by everyone acting on ENAIRE's behalf.

6. APPROVAL AND ENTRY INTO FORCE

Following its presentation to the Management Committee on 9 June 2026, this Policy was approved by ENAIRE's Governing Board at its meeting on 26 June 2026. It entered into force 10 calendar days after approval and superseded the previous 2023 version.

This Policy will remain in force until it is amended, and any amendment will be duly communicated. It will also be reviewed annually and updated where necessary to reflect any regulatory, social, economic or organisational changes.

In accordance with Regulation [\(EU\) 2023/203 \(PART-IS\)](#), this Policy is established and promoted by ENAIRE's Director General in their capacity as *Accountable Manager*.

ENAIRe Director General