facephi

Security Policy Manual

MS-02

Version 10.0

Confidential information

The Facephi logo and all trademarks of "Facephi Biometría S.A." (A-54659313) are registered internationally The names of other products and companies mentioned here may be trademarks of their respective holders for which Facephi has the corresponding authorisation. Because Facephi frequently releases new versions and updates of its software, the images shown in this document may be different from what you see on screen.

Confidentiality declaration

This document contains confidential and proprietary information. All the information presented is provided on the basis of the consent not to use or disclose It, except in commercial agreements with Facephi Biometrics.

The recipient of this document agrees to inform all employees and partners, both current and future, that consult have access to the content of the document, about its confidentiality. The recipient agrees to give precise instructions to employees so that they do not disclose information related to this document, except in the case of matters of public knowledge and that are available for public use. The recipient also agrees not to reproduce or distribute, or permit others to reproduce or distribute, any material contained herein without the express, written consent of Facephi Biometría.

Facephi Biometrics retains all rights of possession and ownership of the material and trademarks contained herein, including supporting documentation, files, marketing material and multimedia.

The acceptance of this document implies that the recipient agrees to be legally bound by the above declaration.

Update board

	Produced by	Approved by
Name	Raúl López	Jorge Sanz
Position	GRC Officer	General Director
Date	12/09/2025	24/09/2025

Versions	Dates	Observations
1.0	26/06/2020	First version
2.0	24/09/2021	ENS adaption
3.0	13/12/2021	New reference to roles and responsibilities
4.0	31/01/2022	Indication of the SGI regulatory scope
5.0	02/08/2022	Incorporation of ISO 27017 for cloud information security
6.0	22/01/2024	Creation of section 5
7.0	22/04/2024	Review after external audit
8.0	07/06/2024	Document review
9.0	29/08/2024	Update of section 1 and 4.1, as well as the SGI Governance organizational chart
10.0	12/09/2025	After external audit, the organizational chart and explicit references to internal documentation are removed. ISO 27701 is added to section 4.1 as a reference and guide for its controls

Contents

1 Scope and Mission

This policy applies to the activities, services, assets, resources, and other parties involved in the provision of products and services by Facephi Biometría S.A.

Facephi adheres to the highest international standards on information security and business continuity, incorporating best practices by implementing controls based on ISO 27001, ISO 27017, ISO 22301, National Security Scheme (ENS), and also takes as reference and guidance controls on privacy management, among others. All this forms the Integrated Management System (SGI).

Facephi has earned the trust of numerous entities globally, involved in handling highly confidential information, thanks to its commitment and effort to ensure the integrity, confidentiality, authenticity, traceability, and availability of information and the systems that support it. Therefore, the objectives of Facephi's SGI are based on the preservation of:

a) Availability, ensuring that authorized users have access to information and its associated assets when required.

b) Confidentiality, ensuring that only those authorized can access the information. Information is not made available or disclosed to unauthorized individuals, entities, or processes. Confidentiality refers to protecting all such data and resources against unauthorized access.

c) Integrity, ensuring that information remains unchanged, i.e., maintaining the accuracy and completeness of information and its methods in the process, guaranteeing that data is reliable and correct, protecting it against unauthorized changes. Integrity is crucial for maintaining information quality.

d) Traceability, ensuring the tracking of who has accessed and/or modified certain information associated with the service.

e) Authenticity, ensuring that whoever accesses the service is indeed who they claim to be, and it is possible to know who has accessed.

From the outset, Information Security and Resilience have been established as value propositions, guaranteeing, in addition to availability, the proper functioning of systems and services, and compliance with any legal, regulatory, or contractual requirements.

Facephi's primary mission has always been to develop technologies for identity verification and authentication, seeking improvement and excellence, aiming to have state-of-the-art algorithms, and for this, it makes a strong investment in R&D to contribute to the evolution of the concept of increasingly secure and resilient digital identity in all its processes.

Key issues include:

a) Preserving and ensuring the integrity of algorithms by analyzing threats that may affect biometrics and thus pose a risk to privacy.
b) Managing and preserving the identity and privacy of data.
c) Ensuring the integrity and quality of the method, as well as the integrity of the code.

The main value of the company is its human value, as it has a committed, proactive team, dedicated to the project and highly motivated.

2 Development

Facephi Management wants to make the SGI Policy known, as its knowledge and understanding are essential for its employees, clients, suppliers, and other stakeholders, since Information Security, Business Continuity, and privacy are key factors for the proper development of the organization.

This Policy demonstrates Management's commitment and has the following high-level objectives:

a) Ensure customer satisfaction by meeting their needs and expectations and preserving the availability, integrity, confidentiality, authenticity, and traceability of information.

b) Demonstrate leadership by ensuring that the Policy and objectives are established and compatible with the organization's strategic direction.

c) Set objectives and goals focused on evaluating performance in Information Security and Business Continuity and improving the activities carried out.

d) Ensure compliance with applicable legislation and regulations, commitments made with clients, and all internal and external standards to which the organization adheres, to achieve continuous improvement.

e) Assign the necessary functions and responsibilities in the field of Information Security and Business Continuity and provide the necessary support.

f) Implement effective and efficient preventive measures in all activities carried out.

g) Establish and periodically review the company's risk appetite, as well as identified risks, their resolution, and/or treatment.

h) Develop, implement, and periodically verify continuity and contingency plans and their associated tests.

i) Train, raise awareness, and motivate staff on the importance of complying with the requirements established in the SGI, both in Information Security and Business Continuity.

j) Maintain smooth communication both internally, among the different levels of the company, and with clients or interested parties.

k) Establish proper documentation structuring as well as adequate management and updating of regulations.

l) Take into account the Information Security and Business Continuity established by its suppliers to guard against possible risks from them.

3 Creation, Update, Approval, and Communication

This document is prepared by the GRC team, with the support and approval of Senior Management.

The Information Manager is responsible for ensuring the suitability and updating of this document. In addition, it is the responsibility of all internal and external personnel related to Facephi to comply with this Policy and ensure its enforcement.

This Policy will be notified to all employees and may be shared with third parties and stakeholders who require it and are present in the execution of activities related to the provision of products and services by Facephi Biometría S.A. Where applicable, it will be included in the training plans for staff and related third parties.

4 Annexes

4.1 Legal and Regulatory Framework

Facephi's legal and regulatory framework is kept up to date and available on the **List of legislation and regulations**. In the field of security, the following stands out:

a) Law 11/2007, of June 22, on electronic access of citizens to Public Services (and subsequent amendments).

b) Royal Decree 311/2022, of May 3, regulating the National Security Scheme in the field of Electronic Administration (and subsequent amendments)

c) Royal Decree 203/2021 of March 30. Regulation of action and operation of the public sector by electronic means (and subsequent amendments).

d) Law 34/2002 of July 11 on information society services and electronic commerce (and subsequent amendments).

e) Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (GDPR) (and subsequent amendments).

f) Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, establishing harmonized rules on artificial intelligence (Artificial Intelligence Regulation).

g) Organic Law on Data Protection and Guarantee of Digital Rights 3/2018 of December 5. (LOPDGDD) (and subsequent amendments).

h) Law 10/2021, of July 9, on remote work (and subsequent amendments).

i) Royal Decree-Law 12/2018, September 7, on the security of networks and information systems (and subsequent amendments).

j) Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption.

k) ISO 27001:2022 Information Security Management Systems. Requirements.

l) ISO 27002:2022 Information Security Controls Framework.

m) ISO 22301:2019 Security and resilience. Business Continuity Management System.

n) ISO 27017:2015 Security Techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

o) ISO 27701:2019 Information security, cybersecurity, and privacy protection - Privacy information management systems - Requirements and guidance.

4.2 Roles and Functions

To demonstrate the organization's commitment and leadership in information security, as well as its maintenance and continuous improvement, the following persons are appointed by Management for the Integrated Management System and the National Security Scheme.

The expansion of each role's functions is described in **Roles, responsibilities, and authorities**.

4.2.1 Security Manager

The Security Manager is appointed by Management and determines decisions to meet information security and service requirements. The two essential functions assigned are:

a) Maintain the security of the information handled and the services provided by the information systems in accordance with this policy.
b) Promote training and awareness in security within their area of responsibility, monitoring and analyzing security alerts and information and distributing it among staff, as well as procedures for response and escalation of security incidents.

4.2.2 System Manager

The System Manager is appointed by Executive Management and has the following assigned functions:

a) Develop, operate, and maintain the information system throughout its lifecycle, including its specifications, installation, and verification of proper operation.
b) Define the topology and management of the information system, establishing usage criteria and available services.
c) Ensure that security measures are properly integrated into the overall security framework.

4.2.3 Information Manager

The Information Manager is appointed by Executive Management and has the following assigned functions:

a) The Information Manager has ultimate responsibility for the use of certain information and, therefore, its protection.
b) Determines the (security) requirements of the information processed, according to the parameters of Annex I of the ENS.
c) The assessment of the consequences of a negative impact on information security will be made considering its impact on the organization's ability to achieve its objectives, asset protection, fulfillment of service obligations, compliance with the law, and citizens' rights.
d) Manages information security risks and acceptance of residual risk, together with Management, being ultimately responsible for any error or negligence leading to a confidentiality or integrity incident (in terms of data protection) and availability (in terms of information security).
d) Ensures the proper establishment of the SGI.

4.2.4 Service Manager

The Service Manager is appointed by Executive Management and has the following assigned functions:

a) The Service Manager has the authority to determine the security levels of services.
b) Include security specifications in the lifecycle of services and systems.
c) Assess the consequences of a negative impact on service security.

4.2.5 Data Protection Officer

The Data Protection Officer is responsible for the following functions:

a) Privacy and data protection.
b) Review and update of the website's legal notice.
c) Control, review, and update of privacy policies (web and demo) and cookie policy.
d) Legal assistance to the technical team in the development of new solutions (data protection).
e) Support to the commercial team in researching international legislation and preparing reports.
f) Drafting and reviewing data processing agreements.

g) Legal support in the supplier approval process.
h) Responsible for agreeing and supervising the execution of impact assessments for the processing of especially protected data when appropriate. In such cases, and together with the technical area, necessary security measures will be adopted to eliminate or minimize identified and analyzed risks.
i) Inform and advise the controller or processor, to process personal data under their direct authority.
j) Act as the contact point for the supervisory authority.

4.3 Security Committees

4.3.1 SGI Corporate Governance

To ensure a high specific weight of Corporate Governance at Facephi, it has the following composition:

- CEO
- General Director
- CTO
- Legal Director
- People & Culture Director

In addition to the permanent members, those whose presence is considered strategically important, both internal and external, may be called to meetings.

This committee will be used to resolve responsibility conflicts that may arise between officers and/or different areas of the organization, escalating those cases where it does not have sufficient authority to decide.

4.3.2 SGI Executive Management

Due to its practical nature, it is made up of the Facephi members most immediately responsible for implementing the guidelines given by Corporate Governance:

- Information Manager
- Systems Manager
- Security Manager
- GRC Manager

As in Corporate Governance, the presence of those members, exclusively from the organization, whose presence is crucial for the definition and execution of any plans to be established, may be called.

For more details on the responsibilities of the bodies that are part of the Security Committee, see the procedure for Roles, responsibilities, and attributions.

5 Security Principles and Requirements

Facephi, in accordance with Article 12 of the National Security Scheme, has established the following basic principles and minimum security requirements:

- Security at Facephi is understood as a comprehensive process consisting of all technical, human, material, and organizational elements related to information systems.

- The security of information systems will cover prevention, detection, and correction aspects of threats to ensure that they do not materialize or affect the information and services provided by Facephi.

- Great importance will be given to raising awareness among those involved in the process and their managers to prevent security risks.

- Access to information systems will be controlled and granted following the principle of "least privilege" and only to strictly necessary users.
- The security of information systems will be attended to, reviewed, and audited by qualified personnel throughout their lifecycle.

- The areas and facilities where information systems are located must remain in controlled areas and have adequate and proportional mechanisms.

- The acquisition of security products and the contracting of security services must be provided at the required security level.

- Facephi personnel, whether internal or external, must be trained and informed of their duties, obligations, and responsibilities regarding security.

- Due attention must be paid to information stored or in transit through portable equipment or devices.

- User activities must be logged, retaining only strictly necessary information, to monitor improper or unauthorized activities.

- Security incidents must be handled according to the incident management procedure. Any employee must report such incidents to security@facephi.com.

- Systems will have backups, and necessary mechanisms will be established to ensure service continuity.

- The system must have a protection strategy consisting of multiple layers of security distributed so that when one is compromised, it is possible to:
  - Gain time for an adequate reaction to incidents
  - Reduce the possibility of systems being compromised as a whole
  - Minimize the final impact on systems

- These lines of defense must consist of organizational, physical, and logical measures.

- Security measures will be periodically reassessed and updated to adapt their effectiveness to the constant evolution of risks and protection systems.

6 Risks Derived from the Processing of Personal Data

To maintain security and prevent processing from violating the provisions of the reference standards, the controller or processor must assess the inherent risks of processing and apply measures to mitigate them, such as encryption. These measures must ensure an adequate level of security, including confidentiality. When assessing the risk in relation to data security, the risks arising from the processing of personal data must be considered, such as accidental or unlawful destruction, loss, or alteration of personal data transmitted, stored, or otherwise processed, or unauthorized disclosure of or access to such data, which may in particular cause physical, material, or non-material damage.

To achieve the intended purpose, the protection of Personally Identifiable Information (PII), ISO 27701 specifies requirements and provides guidance for implementing, maintaining, and improving a Privacy Information Management System (PIMS) as an extension of ISO 27001 for privacy management in the organizational context.

7 Risk Management

Risk analysis and management are essential parts of the security process at Facephi. All systems subject to this Policy must undergo a risk analysis, evaluating the threats and risks to which they are exposed. This analysis must be carried out:

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

The results of the risk analysis must be communicated to the Corporate Governance Committee.

8 Documented Information

The "Documented Information" section aims to establish control over all applicable documentation within the SGI.

The Information Manager, or a person delegated by them, is responsible for managing any tasks related to the preparation, control, and management of documented information.

For more details on this section, see the document control and management document, which covers the most important points:

- Internal source documentation
- Document coding
- Document preparation and approval
- Document review
- Document archiving and distribution
- Control of obsolete documentation

- Record control
- External documentation