November 2025

INFORMATION SECURITY AND PRIVACY MANAGEMENT POLICY

This Corporate Policy on Information Security and Personal Data Privacy Management of Laboratorios Normon, S.A. ("NORMON") expresses the commitment of NORMON's Board of Directors, together with NORMON's General Manager and Information Security Committee, to protect the information and personal data it manages in the course of its activities. This Policy applies to all areas, locations, employees and stakeholders of NORMON, and is based on the requirements and best practices established by the UNE-EN ISO/IEC 27001 and UNE-EN ISO/IEC 27701 standards, the General Data Protection Regulation (GDPR), Organic Law 3/2018 (LOPDGDD), the National Security Scheme (ENS) and other applicable legislation and sectoral regulations.

1. **Definition of Information Security**: For the purposes of this policy and in accordance with the UNE-EN ISO/IEC 27001 standard, information security is understood as the preservation of confidentiality (access only by authorised persons), integrity (accuracy and completeness), availability (access when necessary), authenticity (truthfulness of origin) and traceability (recording and tracking of actions on information) of information assets. In the field of privacy, according to UNE-EN ISO/IEC 27701 and the GDPR, this definition is extended to include the protection of the rights and freedoms of individuals who are the owners of personal data, ensuring lawful, fair and transparent processing.

2. **Information Security and Privacy Objectives**: NORMON's main objective is to guarantee, in line with its strategic business objectives, the protection of its information assets and personal data, ensuring business continuity, the trust of customers, employees and third parties, and compliance with legal, regulatory and contractual requirements. To this end, a framework is established to define and review specific security and privacy objectives, which are specified annually and aligned with the following purposes:
   - To protect the confidentiality, integrity, availability, authenticity and traceability of information.
   - Safeguard personal data against any risk of unauthorised access, alteration, loss or destruction.
   - Ensure continuity, operational resilience and protection of critical services.
   - Promote a culture of security and privacy throughout the organisation.
   - Prevent, detect and respond effectively to security incidents and personal data breaches.
   - Continuously evaluate and improve the Information Security and Privacy Management System (ISMS).

3. **Regulatory Framework:** NORMON undertakes to comply with all applicable legal, regulatory and contractual requirements regarding information security and personal data protection. This includes, among others, the GDPR, the LOPDGDD, the ENS, the NIS2 Directive, as well as the UNE-EN ISO/IEC 27001 and 27701 standards, and any requirements arising from agreements with customers, suppliers or authorities. It is guaranteed that internal policies, procedures and controls are aligned with the current regulatory framework and are reviewed periodically to ensure they remain appropriate.

4. **General Principles:** Actions relating to information security and privacy management at NORMON are based on the following principles:

- Confidentiality: Ensuring that information is only accessible to those who are duly authorised.
- Integrity: Safeguard the accuracy and completeness of information and its processing methods.
- Availability: Ensure that authorised users have access to information and associated assets when required.
- Authenticity: Verify and ensure the identity of users, systems and processes, as well as the veracity of the origin of the information.
- Traceability: Record and track all actions performed on the information, allowing for monitoring and auditing.
- Legality and Transparency: Comply with applicable regulations and ensure transparency in the processing of personal data.
- Data minimisation: Limit the processing of personal data to what is strictly necessary for the stated purposes.
- Proactive Responsibility: Demonstrate the effective application of appropriate technical and organisational measures.
- Risk Management: Identify, assess and address risks that may affect information security and privacy.
- Continuous Improvement: Systematically review and refine the management system.
- Awareness and Training: Promote awareness and involvement of all staff and third parties in matters of security and privacy.

5. **Commitment to Risk Assessment Management, RATs and EIPDs**: In compliance with the GDPR and ISO 27001 and ISO 27701 standards, NORMON systematically carries out risk assessments related to both Information Security and Personal Data Processing Activities (RATs), as well as Data Protection Impact Assessments (DPIAs) when the type of processing requires it or when high risks to the rights and freedoms of data subjects are identified. These activities enable the identification and assessment of the risks inherent in each information asset and personal data processing operation, establishing and applying mitigation measures in accordance with legal requirements and international security and privacy standards. The procedure includes detailed documentation of the results, periodic reviews and updates in the event of significant changes in processing, the regulatory environment or the organisational context. Furthermore, the integration of RATs and DPIs into management processes and the implementation of controls proportionate to the level of risk consolidate NORMON's commitment to effective information protection, regulatory compliance and the adoption of international best practices in security and privacy.

6. **Commitment to Comprehensive Security**: NORMON considers Comprehensive Security to be a fundamental pillar for achieving its objectives, ensuring the protection of information systems through the implementation, development and validation of operational continuity plans that form part of the Business Continuity System. This approach guarantees the availability of critical information and services for customers at all times. This commitment is underpinned by an organisational culture focused on information security and privacy, promoted through training and awareness-raising activities aimed at all staff. Comprehensive Security is managed across the following areas:
   - Physical Security: Protection of facilities, premises, hardware systems, media and any physical assets related to information processing, as well as physical access controls.
   - Logical Security: This includes the defence of applications, networks, electronic communications, computer systems and the corresponding logical accesses.

- Political-Corporate Security: Covers security aspects inherent to the organisation, including internal rules, regulations and compliance with current legislation.

The information managed by NORMON is classified and labelled in the following categories: *public, general confidential, internal confidential, restricted access confidential and internal restricted access confidential*. This classification facilitates the secure management of both internal and external communications, as well as stored and in-transit information, ensuring that each type of data receives a level of protection commensurate with its sensitivity. The technical and organisational measures implemented include: pseudonymisation and data encryption, role-based access control and multi-factor authentication (MFA) policies, secure management of media and devices, activity logging and monitoring, ongoing staff training in data protection, and appropriate management of security incidents. In addition, the integration of the principle of privacy by design and by default is encouraged, ensuring that any new processing or system incorporates appropriate safeguards from its initial phase.

7. **Assignment of Responsibilities and Roles:** Responsibilities regarding information security and privacy are clearly defined and assigned at all levels of the organisation, in accordance with the organisational structure and internal procedures:
   - Board of Directors: Approves the policy and monitors compliance.
   - Senior Management: Leads the implementation and provision of resources for the system management
   - Information Security Committee: Coordinates, evaluates and reviews security and privacy initiatives and controls.
   - Data Protection Officer (DPO): Oversees compliance with data protection regulations, advises and acts as a point of contact with data subjects and authorities.
   - Chief Information Security Officer (CISO): Directs security strategy, manages risks and oversees the implementation of protection controls.
   - Data Manager: Ensures the proper management and protection of data in accordance with current regulations.
   - Head of Digital Transformation: Leads the organisation's digitisation projects, drives the adoption of new technologies and coordinates the integration of innovative solutions to optimise processes, ensure security and promote efficiency in line with strategic objectives.
   - IT Service Security Manager: Responsible for protecting technology systems and services, ensuring their resilience and continuity.
   - OT Service Security Manager: Oversees the security of industrial operational and technological systems.
   - IT Service Management System Manager: Administers and optimises processes related to technology service management.
   - Information Security System Management Officer: Coordinates the maintenance and continuous improvement of the security management system.
   - Department Managers: Ensure the application of policies and procedures within their areas of competence.
   - Employees: They must be aware of and comply with the obligations and best practices established in the policy and procedures. Training and awareness-raising on security and privacy is mandatory and ongoing for all staff, in order to ensure the necessary competence and commitment.

8. **Procedure for Handling Exemptions and Exceptions:** In accordance with Control 5.1 of the UNE-EN-ISO/IEC 27002:2023 Standard, any exemption or exception to this Policy or the

associated procedures must be formally requested by the person responsible for the affected area, justifying the need and scope of the exemption. The procedure shall be as follows:

1) Submission of the duly justified request for exemption or exception to the Information Security Committee.
2) Evaluation of the request by the Committee, considering the risks, impacts and alternative safeguards.
3) Reasoned decision by the Committee, which may approve, reject or request modifications to the request.
4) Documentary record of the authorised exemption or exception, including conditions, timeframe and those responsible for monitoring.
5) Communication of the decision to the interested parties and periodic review of the exemptions granted.

9. **Protection of Stakeholders:** The protection of the personal information and data of customers, suppliers, employees and other stakeholders is a priority for NORMON. To this end, appropriate technical, operational and organisational measures are implemented, as well as specific contractual clauses in relations with third parties. In compliance with the GDPR, we maintain and update the mandatory RATs, ensuring traceability and transparency in the use of personal data. In addition, we develop and maintain an up-to-date Information Security and Privacy Management Manual, which sets out the procedures, technical instructions and controls necessary to ensure security and privacy, in accordance with the structure and requirements of the ISMS.

10. **Continuous Improvement:** NORMON considers continuous improvement of the ISMS to be an essential pillar, through the definition of measurable objectives, monitoring of key indicators, internal and external audits, management reviews and the adoption of best practices in the sector. The effectiveness of the measures implemented is evaluated on a regular basis and improvement actions are established to raise the level of maturity and resilience of the system.

11. **Training and Awareness:** As part of NORMON's information security and privacy management policy, a mandatory and ongoing training and awareness programme is implemented for all staff. This programme aims to ensure that all employees have the up-to-date skills necessary to protect personal data, comply with current regulations, securely manage IT services and use technologies, including artificial intelligence, in an ethical and secure manner. The training is reviewed and updated periodically to respond to regulatory changes, technological advances and organisational changes, thus promoting a corporate culture of security and privacy that is fully aligned with the principles and requirements of the organisation's ISMS.

12. **Applicability, Availability and Dissemination:** This policy is mandatory for all NORMON staff and departments, and is available for consultation at all organisational levels and by interested parties upon request. Its dissemination is guaranteed through corporate channels and the internal document repository, facilitating access for both internal staff and external stakeholders. The policy will be reviewed at least once a year, or whenever there are significant changes in the regulatory, technological or organisational framework, and will be updated based on the results of these reviews and the evolution of the risks detected.

13. **Reflection on Policy Integration or Separation:** Integrating information security and privacy management policies into a common framework offers significant advantages, such as resource optimisation, consistency in the application of controls, and strategic alignment of the organisation's protection objectives. However, it is also important to consider the inherent differences between the two disciplines: while information security encompasses

Protection of all information assets, privacy management focuses specifically on personal data and compliance with associated legal requirements.

14. **Management Commitment:** NORMON's Board of Directors, General Manager and Information Security Committee reaffirm their commitment to leading the implementation of this policy, promoting the participation and responsibility of the entire organisation in order to achieve the established objectives.

Approved by General Manager

November 2025