INFORMATION

SECURITY POLICY

Content

1 Approval and entry into force

Text approved on 13-01-2025 by the Safety Committee of BIOSOFTT INNOVATION SL.

This "Information Security Policy", hereinafter the Policy, will be effective from its date of approval and until it is replaced by a new Policy.

2 Introduction

BIOSOFTT INNOVATION SL depends on ICT (Information and Communication Technologies) systems to achieve its objectives. These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the security of the information processed or the services provided, and always be protected against threats or incidents with the potential to affect the confidentiality, integrity, availability, traceability and authenticity of the information processed and the services provided.

To address these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continued delivery of services. This implies that departments must apply the minimum security measures required by the National Security Scheme (ENS), as well as continuously monitor the levels of service provision, monitor and analyze reported vulnerabilities, and prepare an effective response to cyber incidents to ensure the continuity of the services provided.

In this way, all the administrative units of BIOSOFTT INNOVATION SL are aware that ICT security is an integral part of each stage of the system's life cycle, from its conception to its decommissioning, including development or acquisition decisions and operating activities. Security requirements and funding needs should be identified and included in planning, in the request for proposals, and in tender documents for ICT projects.

Therefore, for BIOSOFTT INNOVATION SL, the objective of Information Security is to guarantee the quality of information and the continuous provision of services, acting preventively, supervising daily activity to detect any incident and reacting promptly to incidents in order to recover services as soon as possible, as established in Article 7 of the ENS. with the application of the measures listed below.

2.1 Prevention

In order to ensure that the information and/or services are not harmed by security incidents, BIOSOFTT INNOVATION SL implements the security measures established by the ENS, as well as any other additional controls, which it has identified as necessary, through a threat and risk assessment. These controls, the safety roles and responsibilities of all personnel, are clearly defined and documented.

To ensure compliance with the policy, BIOSOFTT INNOVATION SL:

- Authorizes systems before they go into operation.
- Regularly assesses security, including analysis of configuration changes made routinely.
- Request periodic review by third parties, in order to obtain an independent evaluation.

2.2 Detection

BIOSOFTT INNOVATION SL establishes operational controls of its information systems with the aim of detecting anomalies in the provision of services and acting accordingly in accordance with the provisions of

article 9 of the ENS (periodic re-evaluation). When there is a significant deviation from the parameters that have been pre-established as normal (as indicated in Article 8 of the ENS, Lines of Defence), the necessary detection, analysis and reporting mechanisms will be established so that they reach those responsible on a regular basis.

2.3 Answer

BIOSOFTT INNOVATION SL will establish the following measures:

- Mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or in other agencies.
- Establish protocols for the exchange of information related to the incident. This includes two-way communications with Emergency Response Teams (CERTs).

2.4 Recovery

To guarantee the availability of services, BIOSOFTT INNOVATION SL has the necessary means and techniques to guarantee the recovery of the most critical services.

3 Mission of BIOSOFTT INNOVATION SL

BIOSOFTT INNOVATION SL provides a biological sample management solution for research, therapeutic and diagnostic purposes called Biosoft SoHo

4 Basic principles

The basic principles are fundamental security guidelines that must always be kept in mind in any activity related to the use of information assets. The following are established:

- Strategic scope: Information security must have the commitment and support of all management levels of BIOSOFTT INNOVATION SL, so that it can be coordinated and integrated with the rest of the organization's strategic initiatives to form a coherent and effective whole.
- Determined responsibility: In ICT systems, the Information Controller will be determined, who determines the security requirements of the information processed; the Service Manager, who determines the security requirements of the services provided; the System Manager, who has responsibility for the provision of services and the Security Officer, who determines decisions to meet security requirements.
- Comprehensive security: Security will be understood as an integral process made up of all the technical, human, material and organisational elements related to ICT systems, trying to avoid any specific action or circumstantial treatment. Information security must be considered as part of the usual operation, being present and applied from the initial design of ICT systems.
- Risk Management: Risk analysis and management will be an essential part of the security process. Risk management will allow the maintenance of a controlled environment, minimizing risks to acceptable levels. The reduction of these levels will be done through the deployment of security measures, which will strike a balance between the nature of the data and processing, the impact and likelihood of the risks to which they are exposed, and the effectiveness and cost of the security measures. When

assessing the risk in relation to data security, the risks arising from the processing of personal data must be taken into account.

- Proportionality: The establishment of protection, detection and recovery measures must be proportional to the potential risks and to the criticality and value of the information and services affected.
- Continuous improvement: Security measures will be re-evaluated and updated periodically to adapt their effectiveness to the constant evolution of risks and protection systems. Information security will be attended, reviewed and audited by qualified, trained and dedicated personnel.
- Security by default: Systems must be designed and configured in such a way as to ensure a sufficient degree of security by default.

5 Objectives of Information Security

BIOSOFTT INNOVATION SL establishes the following information security objectives:

5.1 Strategic objectives

1. ENS Governance and Compliance: **Have and maintain a formally defined security framework aligned with the ENS (security policy, regulations, procedures, and roles), reviewed at least once a year.**
2. Risk Management and Systems Categorization: **Perform and keep updated a formal risk analysis and ENS categorization of all information systems, covering the five dimensions (Confidentiality, Integrity, Availability, Authenticity, and Traceability).**
3. Regulatory compliance (ENS + GDPR/LOPDGDD): **Ensure that the processing of personal data and technical and organisational security simultaneously comply with ENS and data protection regulations (GDPR, LOPDGDD), including privacy by design and by default.**

5.2 Operational/Technical Objectives

1. Confidentiality and access control: **Ensure that access to information is done with the principle of least privilege and robust authentication mechanisms (e.g. MFA), reviewing permissions with a defined periodicity.**
2. Information integrity and change control: **Establish a formal change management process that ensures the integrity of information and systems, including testing, approval, and traceability of all changes in production environments.**
3. Availability and service continuity: **Ensure the availability of critical services through business continuity and disaster recovery plans (BCP/DRP), regular testing, and verified backups.**
4. Traceability and activity logging: Implement and maintain a centralised system for recording and monitoring security events, which ensures the traceability of relevant operations, especially on sensitive information and administration actions.
5. Security incident management**: Have a formal incident management procedure, coordinated with the ENS and public sector clients, that defines detection, classification, response, communication, and lessons learned.**
6. Security in the software and infrastructure lifecycle: **Integrate security controls throughout the development lifecycle (DevSecOps) and in the operation of the infrastructure (hardening, patching, secure configuration).**
7. Supplier and supply chain security: **Ensure that suppliers and subcontractors supporting services covered by ENS meet equivalent security requirements, including contractual agreements, SLAs, and evidence of compliance.**
8. Security awareness and training: **Maintain a continuous security awareness and training program for all personnel, adapted to different profiles (management, IT, development, support, etc.).**

9. Continuous improvement and auditing: **Establish a continuous improvement cycle that integrates results from ENS audits, security reviews, risk analysis, and incidents to update controls and documentation.**

6 Scope

This Policy will apply to the information systems of BIOSOFTT INNOVATION SL related to the exercise of its powers and to all users with authorized access to them, whether or not they are from our organization and regardless of the nature of their legal relationship with BIOSOFTT INNOVATION SL. All of them have the obligation to know and comply with this Information Security Policy and its derived Security Regulations, being the responsibility of the Information Security Committee to provide the necessary means for the information to reach the affected personnel.

7 Regulatory framework

The regulatory framework in which the activities of BIOSOFTT INNOVATION SL are carried out, and, in particular, the provision of its electronic services, is made up of the following rules:

- ✓ Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations and amendments according to RDL 14-2019, of 31 October, on urgent measures for reasons of public security in the field of digital administration, public sector procurement and telecommunications.
- ✓ Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.
- ✓ Royal Decree 311/2022, of 3 May, regulating the National Security Scheme
- ✓ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- ✓ Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights.
- ✓ Royal Legislative Decree 1/1996, of 12 April, approving the Revised Text of the Intellectual Property Law.
- ✓ Municipal Ordinance Regulating the Use of Electronic Administration, of 26 February 2019, of the Madrid City Council.

8 Information Security Organization

8.1 Criteria used for the organization of Information Security

BIOSOFTT INNOVATION SL, taking into account the provisions of the aforementioned Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme (ENS) and the guidelines established in the *CCN-STIC-801 Guide "Responsibilities and Functions in the ENS"*, will undertake the following actions to organise information security:

i. It will designate security roles: Service Managers, Information Managers, Security Managers, System Managers and Data Protection Officers.

ii. It will constitute a consultative and strategic body for decision-making in the field of Information Security. This body will be constituted as a collegiate body and will be called the Information Security Committee. It will be chaired by a natural person who will assume formal responsibility for its acts.

8.2 Information Security Roles and Organs

In BIOSOFTT INNOVATION SL, within the framework of the ENS, the roles and bodies of Information Security will be the following:

- Service Managers and Information Controllers:
  - Head of Services: Enrique Cano Lantero
  - Information Manager: Enrique Cano Lantero
  - Data Protection Officer: Subcontracted to EDORTEAM
  - System Manager: Enrique Cano Lantero
  - Head of Security: Manuel Gómez Cristóbal

  - Information Security Committee:
    - President: Enrique Cano Lantero
    - Secretary: Manuel Gómez Cristóbal

The Information and Services Managers will be summoned by the Presidency depending on the matters to be discussed.

The Information Security Committee will meet, on an ordinary basis, at least once every six (6) months, and may meet extraordinarily, for reasons of urgency and justified cause, in shorter periods.

The Secretary of the Committee shall draw up minutes of the meetings of the Security Committee. The meetings of the Security Committee may be attended in an advisory capacity by the persons deemed appropriate by its Chairman in each case.

8.3 Responsibilities of the roles associated with the National Security Scheme

8.3.1 Responsible for Information and Services

The functions of the Information and Service Managers will be:

- To establish and submit for approval to the Information Security Committee the security requirements applicable to Information (Information security levels) and Services (service security levels), within the framework established in Annex I of Royal Decree 3/2010, of 8 January. They may obtain a proposal from the Security Manager and taking into account the opinion of the System Manager.
- To rule on the rights of access to information and services.
- Accept the levels of residual risk that affect information and services.
- Communicate to the Security Officer any variation with respect to the Information and Services for which he/she is responsible, especially the incorporation of new Services or Information at his/her expense. It will transmit these changes to the Information Security Committee at its next meeting.

8.3.2 Safety Officer

The functions of the Security Manager will be:

- Maintain and verify the appropriate level of security of the Information handled and of the Electronic Services provided by the information systems.
- Promote training and awareness in information security.
- Designate those responsible for the execution of the risk analysis, the Statement of Applicability, identify security measures, determine necessary configurations, prepare system documentation.
- Provide advice for the determination of the System Category, in collaboration with the System Manager and/or Information Security Committee.
- It will participate in the preparation and implementation of safety improvement plans and, where appropriate, in continuity plans, proceeding to their validation.
- Manage external or internal system reviews
- Manage certification processes
- Submit to the Safety Committee the approval of changes and other requirements of the system.

8.3.3 System Manager

The functions of the System Manager shall be:

- Develop, operate and maintain the information system throughout its life cycle, developing the necessary operating procedures.
- Define the topology and management of the Information System by establishing the criteria for use and the services available in it.
- Stop access to information or provision of services if they are aware that they have serious security deficiencies.
- Ensure that specific security measures are properly integrated within the overall security framework.
- Provide advice for the determination of the System Category, in collaboration with the Security Officer and/or Information Security Committee.
- Participate in the preparation and implementation of safety improvement plans and, where appropriate, in continuity plans.
- Carry out, where appropriate, the functions of the system security administrator:
    - The management, configuration and updating, where appropriate, of the hardware and software on which the security mechanisms and services are based.
    - The management of the authorisations granted to users of the system, in particular the privileges granted, including the monitoring of the activity carried out in the system and its correspondence with what is authorised.
    - To approve changes in the current configuration of the Information System.
    - Ensure that established security controls are strictly adhered to.
    - Ensure that the approved procedures for managing the Information System are applied.
    - Supervise hardware and software installations, their modifications and improvements to ensure that security is not compromised and that they comply with the relevant authorisations at all times.
    - Monitor the security status provided by security event management tools and technical audit mechanisms.
    - Inform the Security Officer of any anomaly, compromise or vulnerability related to security.
    - Collaborate in the investigation and resolution of security incidents, from detection to resolution.

When the complexity of the system justifies it, the System Manager may designate the delegated system managers that he or she deems necessary, who will be directly functional dependent on the system and will be responsible within their scope for all those actions delegated to them by the system. In the same way, he may also delegate to other specific functions of the responsibilities attributed to him.

8.3.4 Data Protection Officer

The functions of the Data Protection Officer shall be:

- To inform and advise BIOSOFTT INNOVATION SL and the users who are in charge of the processing, of the obligations incumbent on them by virtue of current regulations on Data Protection.
- Supervise compliance with the provisions of security regulations and the internal policies of BIOSOFTT INNOVATION SL in terms of data protection, including the assignment of responsibilities, awareness and training of the personnel involved in the processing operations, and the corresponding audits.
- Provide any advice requested on the data protection impact assessment and monitor its implementation.
- Cooperate with the Spanish Data Protection Agency when required, acting as a point of contact with it for questions related to data processing.

The Data Protection Officer will perform his/her duties paying attention to the risks associated with the processing operations. To do this, they must be able to:

- Gather information to determine treatment activities.
- Analyse and check the conformity of processing activities.
- Inform, advise and issue recommendations to the controller or the data processor.
- Collect information to monitor the recording of processing operations.
- Advise on the principle of data protection by design and by default.
- Advise on whether or not to carry out impact assessments, methodology, safeguards to be applied, etc.
- Prioritize activities based on risks.
- Advise the Data Controller on areas to be committed to audits, training activities to be carried out and processing operations to dedicate more time and resources

8.4 Information Security Committee

The functions of the Information Security Committee shall be:

- To approve and coordinate the proposals of the Information and Services Managers on the levels of information and service security and to assume the functions of the Information and Services Managers in the actions in which it is considered necessary.
- To address the concerns of the Administration and the different areas regarding Information Security, regularly reporting on the state of information security to the Management.
- Advise on information security matters, whenever required.
- Resolve conflicts of responsibility that may arise between the different managers and/or between different Departments, raising those cases in which they do not have sufficient authority to decide.
- Temporarily assume (until the appointment of the Data Protection Officer) the functions of the latter.
- Promote the continuous improvement of the Information Security management system. To this end, it will be responsible for:
    - Coordinate the efforts of the different areas in the area of information security, to ensure that they are consistent, aligned with the strategy decided on the matter, and avoid duplication.

- Propose plans to improve information security, with their corresponding budgetary allocation, prioritising actions in the field of security when resources are limited.
- Ensure that information security is taken into account in all projects from their initial specification to their commissioning. In particular, it should ensure the creation and use of horizontal services that reduce duplication and support a homogeneous operation of all ICT systems.
- To monitor the main residual risks assumed and recommend possible actions with respect to them.
- Monitor the management of security incidents and recommend possible actions with respect to them.
- Prepare (and regularly review) the Information Security Policy for approval by the Higher Body.
- To prepare the Information Security regulations for approval by the Higher Body.
- Verify information security procedures and other documentation for approval.
- Develop training programmes aimed at training and raising awareness among staff in the field of information security and data protection.
- Develop and approve the training and qualification requirements for administrators, operators and users from the point of view of information security.
- Promote the performance of periodic ENS and GDPR audits to verify compliance with the obligations of BIOSOFTT INNOVATION SL in terms of Information Security and Data Protection.

8.5 Appointment procedures

The creation of the Information Security Committee, the appointment of its members and the designation of the Data Controllers identified in this Policy, will be carried out by the superior body of BIOSOFTT INNOVATION SL.

The appointment will be reviewed.

9 Personal data

BIOSOFTT INNOVATION SL will only collect and process personal data when they are adequate, pertinent and not excessive and these are related to the scope and purposes for which they have been obtained. Likewise, it will adopt the technical and organisational measures necessary to comply with Data Protection regulations.

BIOSOFTT INNOVATION SL will publish its Privacy Policy on the Electronic Office.

10 Staff Duties

All BIOSOFTT INNOVATION SL staff within the scope of the ENS will attend one or more security and data protection awareness sessions, at least once a year. A continuous awareness programme will be established to serve all staff, in particular new recruits.

Persons with responsibility for the use, operation or administration of information systems shall be trained in the safe handling of the systems to the extent that they need it to perform their work. Training will be mandatory before assuming a responsibility, whether it is your first assignment or if it is a change of job or responsibilities in it.

11 Risk Management

All systems affected by this Information Security Policy are subject to a risk analysis in order to assess the threats and risks to which they are exposed. This analysis will be repeated:

- At least once a year.
- When the information and/or services handled change significantly.
- When a serious security incident occurs or serious vulnerabilities are detected.

The Security Officer will be responsible for carrying out the risk analysis, as well as identifying shortcomings and weaknesses and bringing them to the attention of the Information Security Committee.

The Information Security Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

The risk management process will comprise the following phases:

- Categorization of systems.
- Risk analysis.
- The Information Security Committee will proceed to select the security measures to be applied, which must be proportionate to the risks and justified.

The phases of this process will be carried out in accordance with the provisions of Annexes I and II of Royal Decree 3/2010, of 8 January, and following the rules, instructions, CCN-STIC Guides and recommendations for its application prepared by the National Cryptologic Centre.

In particular, a recognised risk analysis and management methodology shall be used as a general rule for carrying out the risk analysis.

12 Incident Reporting

In accordance with the provisions of Article 36 of RD 3/2010, of 8 January, BIOSOFTT INNOVATION SL will notify the National Cryptologic Centre of those incidents that have a significant impact on the security of the information handled and the services provided in relation to the categorisation of systems included in Annex I of said legal body.

13 Development of the Information Security Policy

This Information Security Policy will be complemented by various security regulations and recommendations (security standards and procedures, technical security procedures, reports, records and electronic evidence). The Information Security Committee is responsible for its annual review and/or maintenance, proposing, if necessary, improvements to it.

The body of information security regulations will be developed at three levels by scope of application, level of technical detail and mandatory compliance, so that each standard at a given level of development is based on higher-level standards. These levels of regulatory development are as follows:

a) First regulatory level: constituted by this Information Security Policy, the Internal Regulations on the Use of Electronic Media and the general security guidelines applicable to the bodies or units of BIOSOFTT INNOVATION SL to which these documents apply.
b) Second regulatory level: constituted by the safety standards derived from the previous ones.

c) Third regulatory level: made up of procedures, guides and technical instructions. These are documents that, in compliance with the provisions of the Information Security Policy, determine the actions or tasks to be carried out in the performance of a process.

The superior body of BIOSOFTT INNOVATION SL is responsible for approving the Information Security Policy and the Internal Regulations for the Use of Electronic Media of BIOSOFTT INNOVATION SL, with the Information Security Committee being the body responsible for approving the remaining documents, and is also responsible for their dissemination so that the affected parties are aware of them.

In the same way, this Information Security Policy complements the Privacy Policy of BIOSOFTT INNOVATION SL in terms of data protection.

The security regulations and, in particular, the Information Security Policy and the Internal Regulations for the Use of Electronic Means, will be known and available to all members of the ENTITY/ES, in particular to those who use, operate or manage the information and communications systems. It will be available for consultation on the Intranet, in paper format, this documentation will be kept by the IT Service.

14 Thirds

When BIOSOFTT INNOVATION SL provides services to other bodies or handles information from other bodies, they will be made a party to this Information Security Policy. Channels will be established for the reporting and coordination of the respective Information Security Committees and action procedures will be established for the reaction to security incidents.

When BIOSOFTT INNOVATION SL uses third-party services or transfers information to third parties, they will be made aware of this Security Policy and the security regulations that concern such services or information. This third party will be subject to the obligations established in said regulations, and may develop its own operating procedures to satisfy it. Specific procedures for reporting and resolving incidents will be established. It will be ensured that third-party personnel are adequately aware of security, at least at the same level as that established in this Security Policy.

When any aspect of this Information Security Policy cannot be satisfied by a third party as required in the previous paragraphs, a report from the Security Officer will be required that specifies the risks incurred and the way to deal with them. Approval of this report by those responsible for the information and services concerned will be required before proceeding.

15 Continuous improvement

Information security management is a process that is subject to constant updating. Changes in organization, threats, technologies, and/or legislation are an example where continuous improvement of systems is necessary. For this reason, it is necessary to implement a permanent process that will involve, among other actions:

a) Review of the Information Security Policy.
b) Review of services and information and their categorization.
c) Execution of the risk analysis on an annual basis.
d) Carrying out internal or, where appropriate, external audits.
e) Review of security measures.
f) Review and update of rules and procedures.

16 Modifications

Version	Date	Modifications compared to the previous version
01	13-01-025	Original Document