BIOARRAY Diagnóstico Genético

INFORMATION SECURITY POLICY

[PUBLIC SUMMARY]

Information Security Management System · Spanish National Security Framework (ENS)

1. Approval and entry into force

This Information Security Policy enters into force on the date of its approval by BIOARRAY Management and remains in force until it is replaced by a new version. This document is a public summary of the approved policy.

2. Mission of the organisation

BIOARRAY is a genetic diagnostics and research laboratory specialising in genetic analysis using cutting-edge technologies (NGS, CGH arrays, molecular cytogenetics), serving the medical, research and biotechnology sectors.

Its activity involves processing genetic and health data, which are special categories of personal data. For this reason, information security is an integral part of the quality of the diagnostic service. BIOARRAY's security mission is to protect patients' clinical and genetic data and all the information assets that support its diagnostic and scientific research services, ensuring:

Availability	Integrity	Confidentiality	Authenticity	Traceability
Authorised users can access information when they need it.	Information and its processing methods are accurate and complete.	Only authorised persons can access information.	Whoever accesses information is who they claim to be.	Access to information can be tracked and verified.

Information systems must be managed with due diligence and protected against accidental or deliberate damage. To this end, BIOARRAY acts preventively, monitors day-to-day activity and responds swiftly to incidents. It does so in accordance with the basic principles of the National Security Framework: security as an integral process, risk-based security management, prevention, detection, response and preservation, the existence of lines of defence, continuous monitoring and periodic reassessment, and the separation of responsibilities.

3. Scope

This policy applies to the information systems that store, process and transmit patients' clinical and genetic data and that support BIOARRAY's genetic diagnostics and scientific research services, as well as to the people and other information assets involved in them.

It applies to employees, contractors, suppliers, subcontractors, external collaborators and any third party that accesses information belonging to BIOARRAY or its patients, or that processes, stores, transmits or manages it, whether on the laboratory's premises, remotely or through technology services. Controls are applied proportionately to the type of relationship, the functions performed, the assets accessible and the associated risks.

4. Objectives

Management sets the following information security objectives:

- Guarantee the confidentiality, integrity, availability, authenticity and traceability of patients' clinical and genetic data.
- Ensure the continuity of the diagnostic service and rapid, effective recovery from any incident or contingency.
- Prevent security incidents and reduce the risks arising from the laboratory's activity.
- Comply with applicable legislation, particularly regarding the protection of health and genetic data.
- Foster a cybersecurity culture through staff training and awareness.
- Continuously improve the Information Security Management System.

5. Regulatory framework

BIOARRAY is committed to complying with the applicable legal and regulatory requirements and with the commitments made to patients and clients, and to keeping up to date with any changes to them. The framework within which it carries out its activity includes, among others, the following regulations and references:

- Regulation (EU) 2016/679 (GDPR), in particular Article 9 on genetic and health data.
- Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).
- Royal Decree 311/2022, of 3 May, regulating the National Security Framework (ENS).
- Directive (EU) 2022/2555 (NIS2), on the cybersecurity of essential and important entities.
- UNE-EN ISO 15189:2023, on requirements for quality and competence of medical laboratories.
- Law 6/2020 regulating certain aspects of electronic trust services, and Regulation (EU) 910/2014 (eIDAS).
- Royal Legislative Decree 1/1996, Intellectual Property Law, applicable to R&D&I results.
- CCN-CERT guides (CCN-STIC series) and guidance from the Spanish Data Protection Agency (AEPD) on security breaches.

6. Development and document structure

The policy is developed through a set of documents that help everyone apply it in their work:

- **Security Policy:** this framework of principles and responsibilities.
- **Security regulations:** rules for the use of equipment, services and facilities, and staff responsibilities.
- **Security procedures and guidelines:** instructions on how to operate the system's components securely.
- **Records and evidence:** the outcome of applying the above.

Documentation is stored in BIOARRAY's corporate repository and classified according to its level of confidentiality (public, internal or confidential). Access is granted according to authorised profiles. The Security Officer safeguards and disseminates the approved version. Each document has a code, a version number and an approval date. Obsolete documents are withdrawn and archived. Security records are kept for a minimum of five years, unless applicable legislation establishes a longer period.

7. Security organisation

Ultimate responsibility for information security lies with BIOARRAY Management. Management organises functions and responsibilities, approves the policy and provides the resources needed to achieve the objectives. Managers must lead by example by complying with the established security rules. Management formally appoints the people who hold the following roles:

Role	Main function
Information Owner	Determines the security requirements for the information processed, its classification and its protection throughout its entire life cycle.

Role	Main function
Service Owner	Determines the security requirements for the services provided and ensures their continuity.
Security Officer (RSEG)	Leads and coordinates information security, oversees compliance with the policy, manages incidents and promotes training and awareness.
System Officer (RSIS)	Implements and operates security in the information systems, applies controls and manages vulnerabilities.
Data Protection Officer (DPO)	Oversees the protection of personal data and compliance with privacy legislation.

In accordance with the principle of separation of responsibilities, the Security Officer and the System Officer are different people, with no hierarchical dependency between them.

Conflict resolution

Disagreements between officers are addressed by the Information Security Committee, which decides by majority vote and records its decisions in the minutes. If no agreement is reached, Executive Management issues a binding decision.

8. Information Security Committee and Crisis Committee

The **Information Security Committee** is the collegiate body that governs information security at BIOARRAY. It is chaired by Management, the Security Officer acts as secretary, and its members include the other security officers and the heads of the laboratory's departments. Its functions include:

- Drafting and reviewing the Security Policy.
- Coordinating all security functions.
- Ensuring regulatory compliance.
- Coordinating continuity plans.
- Monitoring residual risks and incident management.
- Promoting audits.
- Approving improvement plans.

The **Crisis Committee**, chaired by Management, is the highest decision-making body in a crisis situation. It speeds up decision-making in the event of incidents that may affect the continuity of the diagnostic service, the confidentiality of patient data or the laboratory's reputation.

9. Risk management

The systems covered by this policy undergo a risk analysis that identifies critical assets, the threats affecting them and their vulnerabilities. The analysis follows recognised methodologies such as MAGERIT and covers the five dimensions of security. It is maintained on an ongoing basis and reviewed:

- at least once a year;
- when there are significant changes in the technological environment;
- when applicable legislation changes.

The Security Committee formally approves the risk analyses. Risks are classified according to their likelihood and impact, and are treated by avoiding, reducing, transferring or accepting them. Executive Management approves the acceptance of residual risk on the Committee's proposal, and that risk is documented and reviewed periodically.

10. Personnel management

All members of BIOARRAY are obliged to know and comply with this Security Policy and the security regulations that implement it. The Security Committee provides the means necessary to ensure that this information reaches everyone concerned.

All staff receive regular cybersecurity training tailored to their roles. Training covers threat identification, good authentication practices, handling of confidential data and incident response. Awareness campaigns are also organised, and the effectiveness of the training is evaluated in order to improve it.

11. Professionalism

System security is the responsibility of qualified staff with training and experience appropriate to their responsibilities. Security functions are expressly assigned to each role. Third parties providing services to BIOARRAY are subject to the security obligations that apply to them, in proportion to their access to information and systems.

12. Authorisation and access control

Access to information systems and patient data is restricted to duly authorised users, processes and devices. Every access is identified and authenticated, and the principles of need-to-know and least privilege are applied. Permissions are granted according to each person's functions and are reviewed periodically.

13. Protection of facilities

The facilities housing the laboratory's information systems and information are protected against unauthorised access, damage and interference. Physical and environmental protection measures are proportionate to the risks identified.

14. Acquisition of security products and contracting of security services

Security is taken into account when acquiring products and contracting technology services. Wherever possible, priority is given to products and services with certified security functionality appropriate to the required level of protection. Security requirements are included in planning and in contract terms.

15. Least privilege and security by default

Systems are designed and configured to offer only the functionality essential to the laboratory's activity. Security is integrated throughout the entire life cycle of the systems, from conception to decommissioning, including development or acquisition decisions and operation.

16. System integrity and updating

Changes to the physical and logical components of the systems are authorised before installation and controlled through a change management process. The security status of the systems is assessed periodically against manufacturers' specifications, vulnerabilities and available updates. Any risk detected is acted upon promptly.

17. Protection of stored information and information in transit

BIOARRAY protects stored information and information travelling through insecure environments, such as laptops, storage media or open networks. To this end, it applies robust cryptographic mechanisms and measures proportionate to the sensitivity of clinical and genetic data.

18. Prevention regarding other interconnected information systems

The systems' perimeter is protected, particularly at connections with public networks. The risks of each interconnection with third-party systems are analysed and its connection point is controlled.

19. Activity logging, detection of malicious code and incidents

BIOARRAY logs user activity to the extent necessary to monitor, analyse and investigate improper or unauthorised actions, so that the person acting can always be identified. It does so in compliance with data protection legislation. It also has mechanisms for detecting and responding to malicious code.

Security incidents are managed through procedures for detection, classification, analysis, resolution, communication to stakeholders and recording of the actions taken. Personal data breaches are notified as required by law. Lessons learned are used to improve security.

20. Business continuity

BIOARRAY has backups and continuity and recovery plans in place so that, in the event of an incident, the laboratory's essential services can continue to operate or be restored as soon as possible. These plans are tested through regular drills and reviewed based on their results.

21. Review and continuous improvement

The Security Committee reviews this policy at least once a year or whenever there are significant changes in the organisation, technology or legislation. Before Management approves it, it is reviewed by the Security Officer and the System Officer.

Compliance is verified through regular internal and external audits. Deviations are addressed with corrective measures and the results are reported to Executive Management. Continuous improvement applies the criteria of the National Security Framework and the CCN-STIC guides.

BIOARRAY Management is committed to providing the resources necessary for information security and to improving it continuously, as a guarantee of trust for patients, healthcare professionals, clients and partners.

Management · BIOARRAY, S.L.