SECURITY POLICY

Created by:	Reviewed by:	Approved by
Security Officer	**Information Officer**	**CEO**
Date: 05/14/2024	Date: 05/14/2024	Date: 05/14/2024

Document Control		
Version	**Modified sections**	**Amendments**
1	NA	New document

INDEX

1. Approval and entry into force 3
2. Organization's Mission 3
3. Scope 4
4. Objectives 4
5. Regulatory Framework 4
6. Development 5
7. Security Organization 6
8. Security Committee 7
9. Risk Management 8
10. Personnel Management 8
11. Professionalism and Security of Human Resources 9
12. Authorization and access control to Information systems 10
13. Product acquisition 10
14. Security by default 11
15. System integrity and updates 11
16. Protection of stored and in-transit information 11
17. Prevention of interconnected information systems. 11
18. Activity logging 12
19. Business continuity 12
20. Continuous improvement of the security process 12
21. Personal data processing 12

1. Approval and entry into force

This Information Security Policy is effective from the date of signing until it is replaced by a new Policy.

2. Organization's Mission

The mission of REVEAL GENOMICS is to revolutionize the use of biomarkers and the development of in vitro diagnostic tests useful in clinical practice in the field of medical oncology. Specifically, the company seeks to decode the molecular information of the tumor before, during, and/or after treatments, using different biological samples to develop innovative tests that, although highly analytically complex, provide easy-to-interpret results. This allows for determining the best treatment option for cancer, contributing to patient well-being and resource optimization.

To achieve its objectives, it is vital to ensure an information security policy that generates trust among all actors, clients, and end-users involved in the company's solutions. In this regard, REVEAL GENOMICS commits to information security, ensuring its proper management to offer all its stakeholders the highest guarantees regarding the security of the information used.

These systems must be diligently managed, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, or confidentiality of the processed information or the services provided.

The objective of information security is to ensure the quality of information and the continuous provision of services by acting preventively, monitoring daily activity, and responding promptly to incidents.

Information and Communication Technology (ICT) systems must be protected against rapidly evolving threats that can impact confidentiality, integrity, availability, intended use, and value of the information and services. To defend against these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continuous provision of services. This implies that departments must implement the minimum security measures required by the National Security Scheme, continuously monitor service levels, follow and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure service continuity.

Different departments must ensure that ICT security is an integral part of each stage of the system's lifecycle, from conception to retirement, through development or acquisition decisions and operational activities. Security requirements and funding needs must be identified for both the developed products and their associated services, as well as for the base software acquired from third parties.

Departments must be prepared to prevent, detect, respond to, and recover from incidents, following Article 8 of the National Security Scheme (Article 8. Prevention, Detection, Response, and Conservation).

3. Scope

This policy applies to all ICT systems of the entity and all members of the organization involved in Services and Projects aimed at the public sector that require the application of the National Security Scheme. Especially, to the "Information Systems for the Reception and Processing of Diagnostic Test Orders for Cancer Patients."

4. Objectives

Based on the above, the Management establishes the following information security objectives:

- ✓ Provide a framework to enhance resilience to effectively respond.
- ✓ Ensure the quick and efficient recovery of services in the event of any physical disaster or contingency that might risk operational continuity.
- ✓ Prevent information security incidents where technically and economically viable, and mitigate the information security risks generated by our activities.
- ✓ Guarantee the confidentiality, integrity, availability, authenticity, and traceability of information.

5. Regulatory Framework

One of the objectives is to comply with applicable legal requirements and any other requirements we subscribe to, as well as the commitments made with clients, ensuring their continuous updating. To this end, the legal and regulatory framework in which we conduct our activities includes:

- ✓ REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data.
- ✓ Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights.
- ✓ Royal Legislative Decree 1/1996, of 12 April, Intellectual Property Law.

- ✓ Law 2/2019, of 1 March, amending the consolidated text of the Intellectual Property Law, approved by Legislative Royal Decree 1/1996, of 12 April, incorporating into Spanish law Directive 2014/26/EU of the European Parliament and of the Council, of 26 February 2014, and Directive (EU) 2017/1564 of the European Parliament and of the Council, of 13 September 2017.

- ✓ Royal Decree 311/2022, of 3 May, regulating the National Security Scheme.

- ✓ Law 34/2002 of July on Information Society Services and Electronic Commerce (LSSI).

- ✓ Law 40/2015, of 1 October, on the Legal Regime of the Public Sector.

- ✓ Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administration.

6. Development

To achieve these objectives, it is necessary to::

- ✓ Continuously improve our information security system.

- ✓ Identify potential threats and their impact on business operations if they materialize.

- ✓ Preserve the interests of its main stakeholders (customers, shareholders, employees, and suppliers), reputation, brand, and value-creating activities.

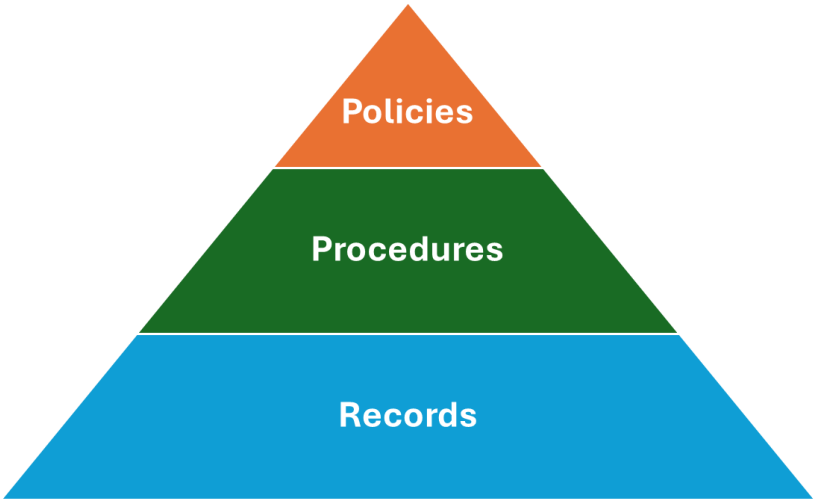
- ✓ Work with our suppliers and subcontractors to improve IT service delivery, service continuity, and information security, enhancing our activity efficiency.

- ✓ Evaluate and ensure the technical competence of personnel and ensure their motivation to participate in the continuous improvement of our processes, providing appropriate training and internal communication to develop best practices defined in the system.

- ✓ Ensure the correct state of facilities and adequate equipment, corresponding with the company's activities, objectives, and goals.

- ✓ Conduct continuous analysis of all relevant processes, implementing necessary improvements based on results and established objectives.
- ✓ Structure our management system to be easy to understand.

  Our management system has the following structure:



The management of our system is entrusted to the Security Officer, and the system will be available in our information system in a repository, which can be accessed according to the access profiles granted as per our current access management procedure.

7. Security Organization

The essential responsibility lies with the organization's General Management, the CEO, who is responsible for organizing functions and responsibilities and providing the appropriate resources to achieve the ENS objectives. Other area managers are also responsible for setting a good example by following the established security rules.

The principles are assumed by the Management, which has the necessary means and provides its employees with sufficient resources for compliance, being embodied and made publicly known through this Security Policy.

The defined security roles or functions are:

Role	Duties and Responsibilities
Information Officer	· Take decisions related to the processed information
Service Officer	· Coordinate the system implementation · Continuously improve the system
Security Officer	· Determine the suitability of technical measures · Provide the best technology for the service
System Officer	· Coordinate the system implementation · Continuously improve the system
Management	· Provide the necessary Resources for the system · Lead the system

This definition of duties and responsibilities is completed in the job profiles and the system documents "Register of Responsibilities, Roles, and Duties."

CONFLICT RESOLUTION:

Differences in criteria that may result in a conflict will be addressed within the Security Committee, and in all cases, the CEO's criteria will prevail.

8. Security Committee

The procedure for the appointment and renewal will be the ratification by the Security Committee.

The committee for managing and coordinating security is the highest authority within the information security management system, making all major decisions related to security.

The members of the Information Security Committee are:

- ✓ Information Officer
- ✓ Service Officer
- ✓ Security Officer

- ✓ System Officer
- ✓ CEO:

These members, except for the CEO, are appointed by the committee, which is the only body that can appoint, renew, and remove them.

The Security Committee is an autonomous, executive body with decision-making autonomy and does not need to subordinate its activities to any other element within our Company. This policy is complemented by the rest of the policies, procedures, and documents in force to develop our management system.

9. Risk Management

All systems subject to this Policy must conduct a risk analysis, evaluating the threats and risks to which they are exposed. This analysis is reviewed regularly:

- ➢ at least once a year;
- ➢ when the information handled changes;
- ➢ when the services provided change;
- ➢ when a serious security incident occurs;
- ➢ when serious vulnerabilities are reported.

To harmonize risk analyses, the ICT Security Committee will establish a reference valuation for the different types of information handled and the different services provided. The ICT Security Committee will facilitate the availability of resources to meet the security needs of the various systems, promoting horizontal investments.

For conducting the risk analysis, the risk analysis methodology developed in the Risk Analysis procedure will be taken into account.

Additionally, the Security Committee will meet annually to review and update, if necessary, the Business Impact Analysis (BIA).

10. Personnel Management

All members of REVEAL GENOMICS are required to be aware of and comply with this Security Policy and the Security Regulations. It is the responsibility of the ICT Security Committee to provide the necessary means to ensure that the information reaches those affected.

All members of REVEAL GENOMICS will attend an ICT security awareness session at least once a year. A continuous awareness program will be established to support all members of REVEAL GENOMICS, particularly new hires.

Individuals responsible for the use, operation, or administration of ICT systems will receive training for the secure handling of systems as needed to perform their work. This training will be mandatory before assuming a responsibility, whether it is their first assignment or a change in job position or responsibilities.

11. Professionalism and Security of Human Resources

This Policy applies to all REVEAL GENOMICS staff and external personnel performing tasks within the Company.

HR, or the person designated by the CEO for this task, will include information security functions in the job descriptions of employees, inform all newly hired personnel of their obligations regarding compliance with the Security Policy, manage Confidentiality Agreements with personnel, and coordinate user training tasks concerning this Policy.

The Security Officer is responsible for monitoring, documenting, and analyzing reported security incidents, as well as communicating with the Information Security Committee and information owners.

The Information Security Committee will be responsible for implementing the necessary means and channels for the Security Management Officer to handle reports of incidents and system anomalies. The Committee will also monitor investigations, oversee the evolution of information, and promote the resolution of information security incidents.

The Security Officer will participate in the preparation of the Confidentiality Agreement to be signed by employees and third parties performing functions at REVEAL GENOMICS, in advising on sanctions to be applied for non-compliance with this Policy, and in handling information security incidents.

All REVEAL GENOMICS personnel are responsible for promptly reporting detected information security weaknesses and incidents.

Professionalism of Human Resources:

- Determine the necessary competence of personnel to carry out work affecting Information Security.
- Ensure that individuals are competent based on appropriate education, training, or experience.
- Demonstrate the necessary competence of personnel in Information Security through documented information.

The objectives of controlling personnel security are:

- Reduce the risks of human error, irregularities, misuse of facilities and resources, and unauthorized handling of information.
- Explain security responsibilities during the recruitment stage and include them in the agreements to be signed, ensuring compliance during the performance of employee tasks.
- Ensure that users are aware of information security threats and concerns and are trained to support the organization's Security Policy in the course of their normal tasks.
- Establish confidentiality agreements with all personnel and users outside the information processing facilities.
- Establish the necessary tools and mechanisms to promote the communication of existing security weaknesses and incidents to minimize their effects and prevent recurrence.

12. Authorization and access control to Information systems

The objective of access control to information systems is:

- ✓ Prevent unauthorized access to information systems, databases, and information services.
- ✓ Implement user access security through authentication and authorization techniques.
- ✓ Control the security of the connection between the REVEAL GENOMICS network and other public or private networks.
- ✓ Review critical events and activities performed by users in the systems.
- ✓ Raise awareness about their responsibility for the use of passwords and equipment.
- ✓ Ensure the security of information when using laptops and personal computers for remote work.

13. Product acquisition

The various departments must ensure that ICT security is an integral part of every stage of the system life cycle, from its conception to its decommissioning, including development or acquisition decisions and operational activities. Security requirements and funding needs

must be identified and included in planning, request for proposals, and bidding documents for ICT projects.

Furthermore, information security will be considered in the acquisition and maintenance of information systems, limiting and managing change.

The policy for the development and acquisition of information systems is detailed in the Policy documents: Acquisition, Development, and Maintenance of Systems.

14. Security by default

REVEAL GENOMICS considers it strategic for the organization that processes integrate information security as part of their life cycle. Information systems and services must include security by default from their creation to their decommissioning, incorporating security into development and/or acquisition decisions and all operational activities, establishing security as an integral and cross-cutting process.

15. System integrity and updates

REVEAL GENOMICS is committed to ensuring system integrity through a change management process that allows for the control of updates to physical or logical components with prior authorization before installation in the system.

The systems management team will assess the impact on system security before making changes and will document and control those changes evaluated as significant or with security implications.

Periodic security reviews will assess the security state of the systems concerning manufacturer specifications, vulnerabilities, and updates affecting them, reacting promptly to manage risk based on the security status of these systems.

16. Protection of stored and in-transit information

REVEAL GENOMICS establishes protective measures for the security of information stored or in transit through insecure environments. Insecure environments are considered to include portable devices, information media, and communications over open networks or with weak encryption.

17. Prevention of interconnected information systems.

REVEAL GENOMICS, establishes protective measures for information security, particularly to protect the perimeter, especially when connecting to public networks, particularly if they are

used wholly or primarily for providing electronic communication services available to the public.
In any case, risks arising from the interconnection of the system, via networks, with other systems will be analyzed, and the connection points will be controlled.

18. Activity logging

REVEAL GENOMICS, will log user activities, retaining the necessary information to monitor, analyze, investigate, and document inappropriate or unauthorized activities, allowing the identification of the individual involved at all times.

19. Business continuity

REVEAL GENOMICS, to ensure continuity of operations, establishes measures to guarantee that systems have backup copies and sets up necessary mechanisms to maintain operational continuity in the event of a loss of regular work resources.

20. Continuous improvement of the security process

REVEAL GENOMICS establishes a continuous improvement process for information security by applying the criteria and methodologies outlined in various standards such as ISO 9001 and ISO 27001.

21. Personal data processing

The processing of personal data involves a series of risks that can affect the rights and freedoms of individuals. These risks can vary, including:

- Confidentiality Breach: Personal data may be accessed, used, or disclosed without authorization by unauthorized third parties.

- Loss of Integrity**:** Personal data may be accidentally or intentionally modified, corrupted, or destroyed.
- Processing Errors: Personal data may be processed incorrectly, inaccurately, or incompletely.

- Lack of Transparency: Data subjects may not be clearly and transparently informed about how their personal data is being processed.

- Discrimination: Personal data may be used to discriminate against individuals based on race, ethnicity, religion, beliefs, political opinions, sex, sexual orientation, disability, or any other legally protected factor.

- Identity Theft: Personal data may be used to impersonate individuals.

- Reputational Damage: Inappropriate processing of personal data can harm the reputation of individuals.

- Civil Liability: Companies may be held liable for damages caused to individuals as a result of inappropriate processing of their personal data.

All personnel at REVEAL GENOMICS are required to comply with the provisions of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 2016 concerning personal data.

Barcelona, May 14, 2024

Patricia Villagrasa-González
CEO & co-founder