Policies and Procedures Manual

Habeas Data

BIO DIAGNOSTICOS S.A.S

Chapter I

Policies and Security of Procedures

1. **Legal base and scope.**

The purpose of the right to Data Protection is to allow all people to know, update and rectify the information that has been collected about them in files or databases. This constitutional right is enshrined in articles 15 and 20 of the Political Constitution; in the Statutory Law 1581 of 2012, which dictates general dispositions for the Personal Data Protection Law (LEPD); in Decree 1074 of 2015, and Chapter 25 Section 3 Article 2.2.2.25.3.2. of the decree1074 of 2015, which partially regulates the 1581 of 2012.

When the Data Subject gives his/her consent for the data to be part of a database of an institution, public or private, legal or natural, this is done through the person responsible for the processing of these data and acquires a series of obligations such as: to treat said data with security and caution, to ensure its integrity and to appear as a body to which the Owner can contact for the monitoring of the information and its control, being able to exercise the rights of consultations and complaints.

Although the responsibility for data processing lies with the data controller, their powers are materialised in the functions that correspond to their service staff. The staff of the institution responsible for the processing with direct or indirect access to databases containing personal data must be aware of the data protection regulations, the data protection policy of the organisation; and must comply with the data security obligations corresponding to their functions and position.

To ensure compliance with its security obligations, the company BIO DIAGNOSTICOS S.A.S, appoints JULISSA VILLAMARIN VERGARA as security officer in charge of developing, coordinating, controlling and verifying compliance with the security measures included in this manual.

This policy shall be applicable to all personal data registered in databases that are processed by the data controller and is aimed at all data users, which are both the own staff and the external staff of the company BIO DIAGNOSTICOS S.A.S**.**

All users identified in this Security document are obliged to comply with the security measures established for the processing of data and are subject to the duty of confidentiality, even after their employment or professional relationship with the organization responsible for the processing has ended. The duty of confidentiality, set out in article 4 literal (h) of the Data Protection Act (LEPD), is formalised through the signing of a confidentiality agreement signed between the user and the data controller.

Type of Rule	Number and issue date	Title	Issued by	Specific Application
Statutory Law	1581 of 2012	*"Through this, general dispositions are dictated for the personal data protection".*	Congress of the Republic.	To develop the constitutional right that all people have to know, update and rectify the information that has been collected about them in databases or files, and the other rights, freedoms and constitutional guarantees to which it refers the article 15 of the Politic Constitution; as well as the right to information enshrined in the article 20 of the same.
Law	1273 of 2009	*Through this, the penal code is modified, is created a new tutored legal asset called "of the protection of the information and data".*	Congress of the Republic.	Through this, the penal code is modified, is created a new tutored legal asset called "of the protection of the information and data" – and are fully preserved systems that use information technologies and communications, among other dispositions.

Decree	1377 of 2013	*'Through this, Law 1581 of 2012 is partially regulated'.*	President of the Republic of Colombia.	Through this, Law 1581 of 2012 is partially regulated. General dispositions are issued for the protection of personal data.
Decree	1074 of 2015	*'Through this is issued the Sole Regulatory Decree of the Commerce, Industry and Tourism sector.*	President of the Republic of Colombia.	The Ministry of Commerce, Industry and Tourism has as its primary objective within its scope: formulate, adopt, direct and coordinate general policies in terms of economic and social development of the country, related to the competitiveness, integration and development of the productive sectors of the industry.

2. Definitions established in article 3 of the LEPD and chapter 25 section 1 article 2.2.2.25.1.3 of Decree 1074 of 2015.

Authorized access: Authorization granted to a user for the use of certain resources. On automated devices it is the result of correct authentication, usually by entering a username and password.

Authentication: Procedure for verifying a user's identity.

Authorization: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

Privacy Notice: Verbal or written communication generated by the data controller, addressed to the Owner for the processing of their personal data, through this the Owner is informed about the existence of the information processing policies that will be applicable to him/her, the way to access them and the purposes of the processing that is intended to be given to the personal data.

Database: Organised set of personal data that is subject to processing.

Password: A secret sign that allows access to devices, information or databases that were previously inaccessible. Used in user authentication that allows authorized access.

Access control: A mechanism that allows access to devices, information or databases through authentication.

Backup: Copy of data from a database on a medium that allows its recovery.

Personal data: Any information linked to or that can be associated with one or more specific or determinable natural persons.

Public data: It is data that is not semi-private, private or sensitive. Public data includes, but is not limited to, data relating to the marital status of persons, their profession or trade and their status as a merchant or public servant. By their nature, public data may be contained, among others, in public registers, public documents, official gazettes and bulletins, and duly enforceable court judgments that are not subject to confidentiality.

Datos sensibles: Sensitive data is understood to be data that affects the privacy of the Owner or whose improper use may lead to discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of trade unions, social or human rights organizations or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sex life, and biometric data.

Treatment Manager: Natural or legal person, public or private, who, by itself or in association with others, processes personal data on behalf of the data controller.

Identification: User identity recognition process.

Incidence: Any anomaly that affects or may affect the security of the data, constituting a risk to the confidentiality, availability or integrity of the databases or the personal data they contain.

User Profile: User group given access.

Protected resource: Any component of the information system, such as databases, programs, media or equipment, used for the storage and processing of personal data.

Security Manager: One or more persons designated by the controller for the control and coordination of security measures.

Information system: Set of databases, programs, media and/or equipment used for the processing of personal data.

Data controller: Natural or legal person, public or private, who by himself or in association with others, decides on the data database and/or the processing of the data.

Support: Material on which information is recorded or on which data can be stored or retrieved, such as paper, videotape, CD, DVD, hard disk, etc.

User: Subject authorized to access data or resources, or process that accesses data or resources without identification of a subject.

Holder: Natural person whose personal data is processed.

Treatment: Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.

Transfer: Data transfer takes place when the controller and/or processor of personal data, located in Colombia, sends the information or personal data to a recipient, who in turn is a controller and is located inside or outside the country.

Transmission: Processing of personal data that involves the communication of such data within or outside the territory of the Republic of Colombia when it is intended to carry out a processing by the processor on behalf of the responsible party.

3. Principles of data protection.

Article 4 of the Data Protection Law (LEPD) establishes principles for the processing of personal data that must be applied, in a harmonious and comprehensive manner, in the development, interpretation and application of the Law. The legal principles of data protection are as follows:

Principle of legality: Data processing is a regulated activity that must be subject to the provisions of the Data Protection Law (LEPD), Decree 1074 of 2015 and other dispositions that develop it.

Principle of purpose: The processing must obey a legitimate purpose in accordance with the Constitution and the Law, which must be informed to the Owner.

Principle of Freedom: The processing may only be carried out with the prior, express and informed consent of the Data Controller. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that discloses consent. The processing of the data requires the prior and informed authorization of the Owner by any means that allows it to be consulted subsequently, except in the following cases that are excepted by article 10 of the Data Protection Law (LEPD):

Information required by a public or administrative entity in the exercise of its legal functions or by court order.

- Data of a public nature.

- Cases of medical health emergency.

Principle of truthfulness or quality: The information subject to processing must be truthful, complete, accurate, updated, verifiable and understandable. The processing of partial, incomplete, fragmented or misleading data is prohibited.

Principle of transparency: In the processing, the right of the Owner to obtain from the person responsible for the treatment or the person in charge of the treatment, at any time and without restrictions, information about the existence of data that concerns him or her must be guaranteed. At the time of requesting authorization from the owner, the person responsible for the treatment must inform him/her clearly and expressly of the following, keeping proof of compliance with this duty:

- The processing to which your data will be subjected and its purpose.

- The optional nature of the Owner's response to the questions asked when they deal with sensitive data or data of children or adolescents.

- The rights that assist him/her as Owner.

- The identification, physical address, email and telephone number of the data controller.

Principle of restricted access and circulation: The processing is subject to the limits arising from the nature of the personal data, the dispositions of the Data Protection Law (LEPD) and the Constitution. In this sense, the processing may only be carried out by authorized persons by the owner and/or by the persons provided for in the Law. Personal data, except for public information, may not be available on the internet and other means of dissemination or mass communication, unless access is technically controllable to provide restricted knowledge only to the Owners or third parties authorized in accordance with the Law.

Principle of security: The information subject to processing by the data controller or data processor must be handled with the technical, human and administrative measures that are necessary to provide security to the records, preventing their adulteration, loss, consultation, use or unauthorized or fraudulent access. The data controller is responsible for implementing the corresponding security measures and for making them known to all personnel who have direct or indirect access to the data. Users who access the data controller's information systems must be aware of and comply with the rules and security measures that correspond to their functions. These rules and security measures are set out in this document, which are mandatory for all users and staff of the company BIO DIAGNOSTICOS S.A.S. Any modification of the rules and measures regarding the security of personal data by the data controller must be made known to the users.

Principle of confidentiality: All persons involved in the processing of personal data that are not public in nature are obliged to guarantee the confidentiality of the information, even after their relationship with any of the tasks included in the processing has ended, and may only provide or communicate personal data when this corresponds to the development of the activities authorized in the LEPD and under the terms of the LEPD.

4. Special categoríes of data.

4.1. Sensitive data.

Sensitive data are those that affect the privacy of the Owner or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership in unions, social organizations, human rights or that promote the

interests of any political party or that guarantee the rights and guarantees of opposition political parties as well as data related to health, sexual life and biometric data.

According to Article 6 of the Statutory Law on the Protection of Personal Data (LEPD), the processing of sensitive data is prohibited, except when:

The Owner has given its explicit authorization to such processing, except in cases where the granting of such authorization is not required by law.

The processing is necessary to safeguard the vital interest of the Owner and he/she is physically or legally incapacitated. In these events, the legal representatives must grant their authorization.

The processing is carried out in the course of legitimate activities and with due guarantees by a foundation, NGO, association or any other non-profit organisation, whose purpose is political, philosophical, religious or trade union, provided that it refers exclusively to its members or to persons who maintain regular contact by reason of its purpose. In these events, the data may not be provided to third parties without the Owner's authorization.

The processing refers to data that are necessary for the recognition, exercise or defence of a right in legal proceedings.

The processing has a historical, statistical, or scientific purpose. In this event, measures must be adopted to suppress the identity of the Holders.

4.2. Rights of children and adolescents

The processing of personal data of children and adolescents is prohibited, except when it is data of a public nature, and when such processing meets the following requirements:

- That responds to and respects the best interests of children and adolescents.

- That their fundamental rights are respected.

Once the above requirements have been met, the legal representative of the child or adolescent shall grant authorization prior to the exercise of the minor's right to be heard, an opinion that shall be assessed taking into account the maturity, autonomy and capacity to understand the matter.

It is the task of the State and educational entities of all kinds to provide information and train legal representatives and guardians on the possible risks faced by children and adolescents with respect to the improper processing of their personal data, and to provide knowledge about the responsible and safe use by children and adolescents of their personal data, their right to privacy and protection of their personal information and that of others.

All persons responsible and in charge involved in the processing of the personal data of children and adolescents must ensure the proper use of the same, complying at all times with the principles and obligations set forth in the LEPD and Decree 1074 of 2015. In any case, the treatment will ensure respect for the prevailing rights of children and adolescents.

The rights of access, correction, deletion, revocation or claim for infringement of the data of children and adolescents will be exercised by the persons who are authorized to represent them.

4.3 Rights of Owners.

In accordance with article 8 of the LEPD and Chapter 25 Section 4 of Decree 1074 of 2015. Data owners may exercise a series of rights in relation to the processing of their personal data. These rights may be exercised by the following persons.

- By the Owner, who must prove his identity sufficiently by the different means made available by the responsible party.

- By their successors, who must prove such quality.

- By the representative and/or attorney of the Owner, after accreditation of the representation or power of attorney.

- By stipulation in favor of another and for another.

- The rights of children or adolescents shall be exercised by persons who are empowered to represent them.

- The rights of the Owner are as follows:

Right of access or consultation: This is the right of the Owner to be informed by the data controller, upon request, regarding the origin, use and purpose that have been given to their personal data.

Complaints and claims rights: The Law distinguishes four types of claims:

Correction claim: The right of the Owner to get updated, rectified or modified data that is partial, inaccurate, incomplete, fragmented, misleading, or data whose processing is expressly prohibited or not authorized.

Deletion claim: The right of the Owner to have data deleted that is inadequate, excessive or that does not respect the constitutional and legal principles, rights and guarantees.

Revocation claim: The right of the Owner to revoke the authorization previously given for the processing of their personal data.

Infringement claim: The Owner's right to request that non-compliance with Data Protection regulations be remedied.

Right to request proof of the authorization granted to the data controller: Except when expressly exempted as a requirement for processing in accordance with the provisions of Article 10 of the LEPD.

Right to file complaints for infringements to the Superintendence of Industry and Commerce: The Owner or successor may only raise this complaint once the consultation or complaint process has been exhausted before the data controller or data processor.

5. Authorization of the treatment policy.

In accordance with Article 9 of the LEPD, the prior and informed consent of the Owner is required for the processing of personal data. By accepting this policy, any Owner who provides information relating to their personal data is consenting to the processing of their data by the company BIO DIAGNOSTICOS S.A.S, under the terms and conditions set out therein.

The Owner's authorisation will not be necessary in the case of:

- Information requested by a public or administrative entity in the exercise of its legal functions or by court order.

- Data of a public nature.

- Cases of medical or health emergency.

- Processing of information authorized by law for historical, statistical or scientific purposes.

- Data related to the Civil Registry of people.

6. Data controller.

The data controller of the databases subject to this policy is the company BIO DIAGNOSTICOS S.A.S., whose contact details are:

Address: AV 6 A NORTE 20 N 53 BRR SANTA MONICA RESIDENCIAL

Email: PROTECDATOS@BIODIAGNOSTICOS.CO

Telephone: (602) 667 2320

6.1. The obligations of the data controller.

The data security obligations of the company BIO DIAGNOSTICOS S.A.S are as follows:

- Coordinate and implement the security measures set out in this document.

- Disseminate the aforementioned document among the affected personnel.

- Keep this Manual updated and revised whenever there are relevant changes in the information system, the processing system, the organisation of the institution, the content of the information in the databases, or as a result of the periodic controls carried out. Similarly, its content will be reviewed when there are any changes that may affect compliance with security measures.

- Designate one or more security officers and identify the users authorized to access the databases.

- Ensure that access through computer systems and applications is carried out through identified access and password.

- Authorize, unless expressly delegated to authorized users identified in this Manual, the departure of media outside the establishments where the databases are located, information inputs and outputs over the network, through electronic or paper storage devices, and the use of modems and data downloads.

- Verify the correct application of the backup and data recovery procedure every six months.

- Ensure that a list of authorized users and user profiles is in place.

- Analyze, together with the corresponding security manager, the incidents recorded to establish the appropriate corrective measures, at least every two months.

- Carry out an audit, internal or external, to verify compliance with data protection security measures, at least every year.

7. Treatment and purposes of the databases

The company BIO DIAGNOSTICOS S.A.S., in the development of its activities, carries out the processing of personal data relating to natural persons that are contained and processed in databases intended for legitimate purposes, in compliance with the Constitution and the Law.

In accordance with the provisions of Law 1581 of 2012 and in accordance with the authorizations given by the owners of the information, the company BIO DIAGNOSTICOS S.A.S will carry out operations or set of operations that include data collection, storage, use, circulation and/or deletion, delivery of data to third parties as processors or responsible parties; this in accordance with the agreement reached between the parties. This Data Processing will be carried out exclusively for the purposes authorised and provided for in this Policy and in the specific authorisations granted by the owner. In the same way, Personal Data Processing will be carried out when there is a legal or contractual obligation to do so, always under the guidelines of the Information Security policies of the company BIO DIAGNOSTICOS S.A.S, in all cases the personal data may be processed in order to carry out the control processes and internal and external audits and evaluations carried out by the control bodies. Likewise, and in execution of the corporate purpose of the company BIO DIAGNOSTICOS S.A.S, the personal data will be processed in accordance with the interest group and in proportion to the purpose or purposes of each processing, as described below:

The following table presents the different databases and the purposes assigned to each of them.

TABLE I. DATABASES AND PURPOSES

COLLABORATORS

The data will be used for the following purposes: Request for data concerning personal identification, contact information, Academic data, Work history, Professional and financial data; Properly develop the registration and employment process; Implement labor welfare actions; disseminate job offers to participate in internal selection processes; Communicate institutional information; To carry out activities for statistical purposes; Properly develop the process of updating the data; Develop the registration processes for congresses; Organized events or seminars; Advance the updating of data and verification of the identity of workers and their relatives (partner, parents, children, economic dependents); Summon applicants in the selection process to scheduled interviews; Carrying out home visits, Verification of work and personal references, work experience, professional trajectory and receipt of resumes of workers or applicants; Provision of information to companies with which it has an agreement, Preparation of equipment items, Sending of information through text messages and emails, Delivery and assignment of equipment to collaborators; Drafting of human management reports; Process of affiliation to the social security system and compensation funds of the collaborator and his beneficiaries; Delivery of work references, Use of photographic images and videos for corporate purposes, Obtaining and providing data of the children of colaborators in the development of recreational and welfare activities through the Institutions or allied entities, Performance evaluations; Generation of labor certifications, promotion, transfer, retirement interview, in audit and internal and external control processes, in the delivery of mandatory institutional reports in retirement interviews, Deactivation of information systems; Use of fingerprints and other health data and/or sensitive data for missionary purposes; The above purposes are illustrative and not exhaustive.

SUPPLIERS

The data will be used for the following purposes: Request for offers and economic proposals for the acquisition of products and services; for the analysis and feasibility of each product and/or service; sending communications via text message and email; submission of relevant reports to the different control entities; review and verification of business references; pre-contractual and contractual procedures; provision of information in internal and external audit processes carried out within the institution; sending information about the Foundation's products, services or news; tracking in restrictive databases such as (police, prosecutor's office, comptroller's office, SARLAFT – Money Laundering and Terrorist Financing Risk Management System and others that Colombian regulations provide) the above purposes are illustrative and not exhaustive.

CLIENTS

The data will be used for the following purposes: It contains customer information; Validations and analyses related to the Money Laundering Risk Management System and against the Financing of Terrorism SAGRLAFT, the prevention against transnational bribery and the others that Colombian regulations provide; in the transmission of data to the entities that regulate the business in tax and customs matters; manage procedures such as requests, complaints and/or claims, reports to risk centers for non-compliance with financial obligations arising from the commercial relationship, sending communications through text messages and emails; to keep a consumption history, Use of photographic images and videos for corporate purposes, Commercial management, Know information on the behavior of store customers, institutional and E-commerce customers and their contact channels to make offers tailored to their needs; sending information on the company's products, services or news, Keeping historical records and maintaining commercial contact; The information granted and authorized by the owner will be sent to the entities with which there are agreements, these transfers will always be mediated by a document that guarantees that the treatment that will be given to their data will be that mandated by current regulations. The above purposes are illustrative and not exhaustive.

PARTNERS

The data will be used for the following purposes: It contains the information of the members; Validations and analyses related to the Money Laundering Risk Management System and against the Financing of Terrorism SAGRLAFT, the prevention against transnational bribery and the others that Colombian regulations provide; in the transmission of data to the entities that regulate the business in tax and customs matters; manage procedures such as requests, complaints and/or claims, reports to risk centers for non-compliance with financial obligations derived from the commercial relationship, sending communications through text messages and emails; to keep a consumption history, Use of photographic images and videos for corporate purposes, Commercial management, To know information on the behavior of the members; sending information about the company's products, services or news, Keeping historical records of the company and maintaining commercial contact; The information granted and authorized by the owner will be sent to the entities with which there are agreements, these transfers will always be mediated by a document that guarantees that the treatment that will be given to their data will be that mandated by current regulations. The above purposes are illustrative and not exhaustive.

7. 1 Attention to Data Owners

JULISSA VILLAMARIN VERGARA, will be in charge of attending to requests, queries and claims before which the owner of the data can exercise their rights, at the following email: PROTECDATOS@BIODIAGNOSTICOS.CO

8. Procedures for exercising the Owner's rights.

8.1. Right of access or consultation.

According to chapter 25 section 4 of decree 1074 of 2015, the Owner may consult his/her personal data free of charge in two cases:

- At least once every calendar month.

- Whenever there are substantial modifications to the information processing policies that motivate new consultations.

- For consultations whose frequency is greater than one per calendar month, the company BIO DIAGNOSTICOS S.A.S, may only charge the Owner for postage, reproduction and, where appropriate, certification of documents. The costs of reproduction may not be greater than the costs of recovering the corresponding material. To this end, the person responsible must demonstrate to the Superintendence of Industry and Commerce, when it so requires, the support of said expenses.

- The Data Owner may exercise the right of access or consultation of their data by writing to the company BIO DIAGNOSTICOS S.A.S, sent by the email PROTECDATOS@BIODIAGNOSTICOS.CO, indicating in the subject "exercise of the right of access or consultation" the request must contain the following data:

- Name and surname of the Owner.

- Photocopy of the Owner's Citizenship Card and, if applicable, of the person representing him/her, as well as the document accrediting such representation.

- Petition in which the request for access or consultation is specified.

- Address for notifications, date and signature of the applicant.

- Documents accrediting the request made, when applicable.

- The Owner may choose one of the following ways of consulting the database to receive the requested information:

- On screen display.

- In writing, with a copy or photocopy sent by certified mail or not.

- Mail or other electronic means.

- Another system suitable for the configuration of the database or the nature of the processing, offered by the company BIO DIAGNOSTICOS S.A.S.

Once the request has been received, the company BIO DIAGNOSTICOS S.A.S. will resolve the request for consultation within a maximum period of ten (10) business days from the date of receipt of the request. When it is not possible to respond to the query within said term, the interested party will be informed, stating the reasons for the delay and indicating the date on which their query will be answered, which in no case may exceed five (5) working days following the expiration of the first term. These deadlines are set out in Article 14 of the LEPD.

Once the consultation process has been exhausted, the Owner or successor may file a complaint with the Superintendence of Industry and Commerce.

8.2. Complaints and claims rights.

The Data Owner may exercise the rights of claim over his/her data by writing to the company BIO DIAGNOSTICOS S.A.S sent, by email to PROTECDATOS@BIODIAGNOSTICOS.CO indicando en el asunto “ejercicio del derecho queja o reclamo”, la solicitud deberá contener los siguientes datos:

- Name and surname of the Owner.

- Photocopy of the Owner's Citizenship Card and, if applicable, of the person representing him/her, as well as the document accrediting such representation.

- Description of the facts and petition in which the request for correction, deletion, revocation or inflation is specified.

- Address for notifications, date and signature of the applicant.

- Documents accrediting the request made that you want to assert, when applicable.

If the claim is incomplete, the interested party will be required within five (5) days of receipt of the claim to correct the defects. If two (2) months have elapsed from the date of the request, without the applicant submitting the required information, it will be understood that the claim has been withdrawn.

Once the complete claim is received, a legend will be included in the database that says "claim in process" and the reason for it, within a term of no more than two (2) business days. This legend must be maintained until the claim is decided. The company BIO DIAGNOSTICOS S.A.S., will resolve the consultation request within a maximum period of fifteen (15) business days from the date of receipt of the same. When it is not possible to address the claim within said term, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.

Once the claim process has been exhausted, the Owner or successor may file a complaint with the Superintendence of Industry and Commerce.

9. Security measures

The company BIO DIAGNOSTICOS S.A.S, in order to comply with the principle of security enshrined in article 4 letter g) of the LEPD, has implemented technical, human and administrative measures necessary to guarantee the security of the records by preventing their adulteration, loss, consultation, use or unauthorized or fraudulent access.

On the other hand, the company BIO DIAGNOSTICOS S.A.S, by signing the corresponding transmission contracts, has required the data processors with whom it works to implement the necessary security measures to guarantee the security and confidentiality of the information in the processing of personal data.

The security measures implemented by the company BIO DIAGNOSTICOS S.A.S, which are included and developed in this document (Tables II, III, IV and V), are set out below.

TABLE II. COMMON SECURITY MEASURES FOR ALL TYPES OF DATA (PUBLIC, SEMI-PRIVATE, PRIVATE, SENSITIVE) AND DATABASES (AUTOMATED, NON-AUTOMATED)

Audit

- Ordinary audit (internal or external) every year.

- Eventual extraordinary audits due to substantial modifications in the information systems.

- Report on the detection of deficiencies and proposal of corrections.

- Analysis and conclusions of the security officer and the data controller.

- Keeping the Report at the disposal of the authority.

Document and media management.

- Measures such as paper shredding that prevent improper access or recovery of data that has been discarded, deleted or destroyed.

- Restricted access to where data is stored.

- Labelling system or identification of the type of information.

- Inventory of the media on which databases are stored.

- Authorisation from the person in charge for the departure of documents or media by physical or electronic means.

Access control

- Limited user access to the data necessary for the development of their functions, according to the role they play.

- Updated list of users and authorized access.

- Written authorisation from the owner of the information for the delivery of their data to third parties, to prevent access to data with rights other than those authorised.

- Granting, altering or cancelling permits by authorised personnel.

Incidents

- Incident register: type of incident, time at which it occurred, issuer of the notification, recipient of the notification, effects and corrective measures.

- Procedure for notification and management of incidents.

Personnel

- Definition of the functions and obligations of users with access to data.

- Definition of the control functions and authorisations delegated by the data controller.

- Dissemination among staff of the rules and the consequences of non-compliance with them.

Policies and Procedures

- Preparation and implementation of the Manual of mandatory compliance for personnel.

- Minimum content: scope of application, security measures and procedures, functions and obligations of staff, description of databases, procedure for incidents, procedure for copying and retrieving data, security measures for the transport, destruction and reuse of documents, identification of data processors.

TABLE III. COMMON SECURITY MEASURES FOR ALL TYPES OF DATA (PUBLIC, SEMI-PRIVATE, PRIVATE, SENSITIVE) ACCORDING TO THE TYPE OF DATABASES

NON-AUTOMATED DATABASES

Archive

Archiving of documentation following procedures that guarantee correct conservation, location and consultation and exercise of the rights of the Owners.

Document storage.

Storage devices with mechanisms that prevent access by unauthorized persons.

Document custody

Duty of diligence and custody of the person in charge of documents during the review or processing of these.

AUTOMATED DATABASES

Identification and authentication

1. Personalized identification of users to access information systems and verification of their authorization.

2. Identification and authentication mechanisms; Passwords: Assignment, Expiration, and Encrypted Storage.

Telecommunications

Data access via secure networks.

TABLE IV. SECURITY MEASURES FOR PRIVATE DATA ACCORDING TO THE TYPE OF DATABASES

AUTOMATED AND NON-AUTOMATED DATABASES

Audit

- Ordinary audit (internal or external) every year.

- Eventual extraordinary audits due to substantial modifications in the information systems.

- Report on the detection of deficiencies and proposal of corrections.

- Analysis and conclusions of the security officer and the data controller.

- Keeping the Report at the disposal of the authority.

Security Manager

- Designation of one or more security officers.

- Designation of one or more persons responsible for the control and coordination of the measures of the Manual, policies and procedures.

- Prohibition of delegation of responsibility from the data controller to the security officer.

Habeas Data Policies and Procedures

- Compliance controls at least once a year, consisting of the annual audit, as well as training of personnel at least once a year.

AUTOMATED DATABASES

Gestión de documentos y soportes

Record of entry and exit of documents and supports: date, sender and receiver, number, type of information, method of delivery, person responsible for reception or delivery.

Access control

Access control to the place or places where the information systems are located.

Identification and authentication

Mechanism that limits the number of repeated unauthorized access attempts..

Incidents

Record of data recovery procedures, person executing them, restored data, and manually recorded data.

Authorisation of the data controller for the execution of recovery procedures.

TABLE V. SECURITY MEASURES FOR SENSITIVE DATA ACCORDING TO THE TYPE OF DATABASES

NON-AUTOMATED DATABASES

Access control

- Access only for authorized personnel.

- Access identification mechanism.

- Logging of unauthorized user access.

Document storage

- Filing cabinets, cabinets or others located in access areas protected with keys or other measures.

Copying or reproduction

- Authorized users only.

- Destruction that prevents access or recovery of data.

Transfer of documentation

- Measures that prevent access to or manipulation of documents.

AUTOMATED DATABASES

Document and media management

- Confidential labeling system.

- Data encryption.

- Encryption of portable devices when they are retired.

Access control

- Access log: user, time, database accessed, type of access, record accessed.

- Control of the access log by the security manager. Monthly report.

- Data retention: for the period imposed by law.

Telecommunications

- Data transmission via encrypted electronic networks.

9.1. Security Officers

Security officers have the following functions:

Coordinate and control the implementation of security measures and collaborate with the data controller in the dissemination of the Habeas Data Policies and Procedures manual.

Coordinate and control the mechanisms that allow access to the information contained in the databases and prepare a periodic report on such control.

Manage data access permissions by authorized users identified in this manual.

Enable incident logging for all users to report and log data security-related incidents; as well as agree with the data controller on corrective measures and record them.

Periodically check the validity of the list of authorized users, the existence and validity of backups for data recovery, the updating of this manual and compliance with the measures related to data inputs and outputs.

Define the times within which the audits will be carried out, which may NOT exceed one year.

Receive and analyse the audit report to raise its conclusions and propose corrective measures to the data controller.

Manage and control records of entries and exits of documents or media containing personal data.

9.2. Users

All persons involved in the storage, processing, consultation or any other activity related to the personal data and information systems of the company BIO DIAGNOSTICOS S.A.S, must act in accordance with the functions and obligations set out in this section.

The company BIO DIAGNOSTICOS S.A.S, complies with the duty of information with its inclusion of confidentiality agreements and duty of secrecy subscribed, where appropriate, by users of identification systems on databases and information systems, and by means of an informative circular addressed to them.

The functions and obligations of the staff of the company BIO DIAGNOSTICOS S.A.S are defined, in general, according to the type of activity they carry out in accordance with their functions within the institution and, specifically, by the content of this Manual. The list of users and profiles with access to protected resources is contained in this document.

In general, when a user processes documents or media containing personal data, he or she has the duty to safeguard them, as well as to monitor and control that unauthorized persons cannot have access to them.

Failure to comply with the obligations and security measures established in this manual of Habeas Data Policies and Procedures. by the staff at the service of the company BIO DIAGNOSTICOS S.A.S, is punishable in accordance with the regulations applicable to the legal relationship between the user and the organisation.

The functions and obligations of the users of the personal databases under the responsibility of the company BIO DIAGNOSTICOS S.A.S. are the following:

Duty of secrecy: It applies to all persons who, in the course of their profession or work, access personal databases and links both users and contracted service providers; in compliance with this duty, the users of the company BIO DIAGNOSTICOS S.A.S may not communicate or disclose to third parties, data that they handle or of which they become aware in the performance or charge of their functions, and must ensure the confidentiality and integrity of this data.

Control functions and delegated authorizations: The data controller may delegate the processing of data to third parties, to act as a processor, by means of a data transmission contract.

Obligations related to the security measures implemented: Access the databases only with due authorization and when necessary for the exercise of their functions.

- Do not disclose information to third parties or unauthorized users.

- Observe safety regulations and work to improve them.

- Do not carry out actions that pose a danger to the security of information.

- Do not take information from the organization's facilities without proper authorization.

Use of resources and work materials: It must be oriented to the exercise of the assigned functions. The use of these resources and materials for personal purposes or unrelated to the tasks corresponding to the job is not authorised. When, for justified work reasons, the exit of peripheral or removable devices is necessary, the corresponding security officer must be notified, who may authorise it and, where appropriate, register it.

Using printers, scanners, and other copying devices: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

Obligation to report incidents: Users are obliged to report any incidents of which they are aware to the corresponding security officer, who will be responsible for their management and resolution. Some examples of incidents are: the failure of the computer security system that allows access to personal data to unauthorized persons, the unauthorized attempt to leave a document or medium, the loss of data or the total or partial destruction of media, the change of physical location of databases, the knowledge of passwords by third parties, the modification of data by unauthorized personnel, etc.

Duty of custody of the media used: It obliges the authorized user to monitor and control that unauthorized persons access the information contained on the media. The media that contain databases must identify the type of information they contain through a labeling system and be inventoried. When the information is classified with a sensitive security level, the labeling system must only be understandable to users authorized to access said information.

Responsibility for workstations and laptops: Each user is responsible for their own workstation; when you are absent from your workstation, you must lock said terminal (e.g. screen saver with password) to prevent viewing or access to the information it contains; and has the duty to turn off the terminal at the end of the working day. Likewise, laptops must be controlled at all times to prevent their loss or theft.

Limited use of the Internet and email: The sending of information electronically and the use of the Internet by staff is limited to the performance of their activities.

Password safeguarding and protection: Passwords provided to users are personal and non-transferable, so their disclosure or communication to unauthorized persons is prohibited. When the user logs in for the first time with the assigned password, it is necessary to change it. When password reset is required, the user must notify the system administrator.

Data backup and recovery: All information in the institution's personal databases must be backed up.

Duty to archive and manage documents and media: Documents and media must be properly filed with the security measures set out in this manual.

10. Transfer of data to third countries.

In accordance with Title VIII of the LEPD, the transfer of personal data to countries that do not provide adequate levels of data protection is prohibited. It is understood that a country offers an adequate level of data protection when it complies with the standards set by the Superintendence of Industry and Commerce on the matter in accordance with circular 005 of August 10, 2017, which in no case may be lower than those required by this law to its recipients. This prohibition shall not apply in the case of:

- Information for which the Owner has granted its express and unequivocal authorization for the transfer.

- Exchange of medical data, when required by the Owner's processing for reasons of public health or hygiene.

- Bank or stock transfers, in accordance with the applicable legislation.

- Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.

- Transfers necessary for the execution of a contract between the Owner and the person responsible for the treatment, or for the execution of pre-contractual measures as long as the Owner's authorization is available.

- Transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defence of a right in a judicial process.

In cases not contemplated as exceptions, it will be the responsibility of the Superintendence of Industry and Commerce to issue the declaration of conformity regarding the international transfer of personal data. The Superintendent is empowered to request information and carry out the proceedings aimed at establishing compliance with the assumptions required for the viability of the operation.

International transfers of personal data that are made between a controller and a processor to allow the processor to carry out the processing on behalf of the controller, will not require the Owner to be informed or have their consent, provided that there is a personal data transfer contract.

.

Chapter II

About Security Measures

1. Compliance and Updating.

This is an internal document that must be complied with by all the company BIO DIAGNOSTICOS S.A.S., personnel, with access to the information systems that contain personal data.

This manual of Habeas Data Policies and Procedures must be subject to permanent review and updating whenever there are changes in the information systems, the processing system, the organization or the content of the information in the databases, which may affect the security measures implemented. Likewise, the manual must be adapted at all times to the legal regulations on the security of personal data.

2. Security measures.

The databases are accessible only by the persons designated by the company BIO DIAGNOSTICOS S.A.S, and referred to in numeral 12 of this document.

The security managers of the company BIO DIAGNOSTICOS S.A.S, indicated in numeral 12 of this manual, are in charge of managing the access permissions to users, the assignment and distribution procedure that guarantees the confidentiality, integrity and storage of passwords, during their validity, as well as the periodicity with which they are changed.

The security measures implemented by the company BIO DIAGNOSTICOS S.A.S, are listed and detailed below.

2.1 Common security measures.

2.1.1 Document and media management.

The documents and media on which the databases are located are determined in the inventory of documents and media.

Those in charge of monitoring and controlling that unauthorized persons cannot access documents and media with personal data are the users authorized to access them. Authorized users are referred to in numeral 12 on databases and information systems of this manual.

Documents and media must classify the data according to the type of information they contain, be inventoried and be accessible only by authorized personnel, unless the characteristics of these make the aforementioned identification impossible, in which case a reasoned record will be left in the log of entry and exit of documents of this manual.

The identification of documents and media containing sensitive personal data must be carried out using understandable and meaningful labelling systems that allow authorised users to identify their content and make identification difficult for other people.

The departure of documents and media containing personal data outside the premises under the control of the data controller must be authorised by the latter. This provision is also applicable to documents or media attached and sent by e-mail.

The inventory of documents and supports of the company BIO DIAGNOSTICOS S.A.S must be included as an annex to this manual.

3. Access control.

The staff of the company BIO DIAGNOSTICOS S.A.S should only access those data and resources necessary for the performance of their functions and for which they are authorised by the data controller in this manual.

The company BIO DIAGNOSTICOS S.A.S. takes care of the storage of an updated list of users, user profiles, and authorized access for each of them. In addition, it has mechanisms to prevent access to data with rights other than those authorized. In the case of computer media, it may consist of assigning passwords, and in the case of documents, handing over keys or mechanisms for opening storage devices where the documentation is stored.

The modification of any data or information, as well as the granting, alteration, inclusion or cancellation of authorized accesses and users included in the updated list mentioned in the previous paragraph, corresponds exclusively to authorized personnel.

Any personnel outside the company BIO DIAGNOSTICOS S.A.S., who, in an authorized and legal manner, have access to the protected resources, will be subject to the same conditions and will have the same security obligations as the company's personnel.

The authorized users to access the databases are established in numeral 6 of this manual.

3.1 Execution of processing outside the institution.

The storage of personal data of the data controller or processor on portable devices and their processing outside the natural place of work, requires prior authorization by the company BIO DIAGNOSTICOS S.A.S., and compliance with the security guarantees corresponding to the processing of this type of data.

3.2 Temporary databases, copies and reproductions.

Temporary databases or copies of documents created for temporary or ancillary work must comply with the same level of security as the original databases or documents. Once they are no longer needed, these temporary databases or copies are deleted or destroyed, thus preventing access or retrieval of the information they contain.

Only the personnel authorized in paragraph 12 may make copies or reproduce the documents.

3.3 Security officer.

In accordance with data protection regulations, the designation of security officers does not exonerate the controller or processor from liability.

4. Audit.

Databases containing personal data, subject to processing by the company BIO DIAGNOSTICOS S.A.S, classified as sensitive or private security level, must be audited every year, this may be an internal or external audit that verifies compliance with the security measures contained in this manual.

Both information systems and data storage and processing facilities will be subject to audit.

The company BIO DIAGNOSTICOS S.A.S., will carry out an extraordinary audit whenever substantial modifications are made to the information system that may affect compliance with security measures, in order to verify their adaptation, adequacy and effectiveness.

The audits will conclude with an audit report that will contain:

- The opinion on the adequacy of the measures and controls to the regulations on data protection.

- The identification of the deficiencies found and the suggestion of necessary corrective or complementary measures.

- A description of the data, facts and observations on which the proposed opinions and recommendations are based.

The corresponding security officer will study the report and transfer the conclusions to the data controller so that he can implement corrective measures. The audit reports will be attached to this manual and will be made available to the Supervisory Authority.

5. Security measures for non-automated databases.

5.1 Document archiving.

The company BIO DIAGNOSTICOS S.A.S, establishes the criteria and procedures of action that must be used for the filing of documents containing personal data in accordance with the Law. The archiving criteria guarantee the conservation, location and consultation of the documents and make possible the rights of consultation and complaint of the Owners. These criteria and procedures are set out in paragraph 12 of this manual.

It is recommended that documents be archived considering, among others, criteria such as the degree of use of users with authorized access to them, the timeliness of their management and/or processing, and the differentiation between historical databases and databases of administration or management of the institution.

Document storage devices must have keys or other mechanisms that make it difficult to open them, except when the physical characteristics of the same prevent it, in which case the company BIO DIAGNOSTICOS S.A.S. will adopt the necessary measures to prevent access by unauthorized persons.

The devices are identified and described in paragraph 12 of this manual.

When documents containing personal data are in the process of being reviewed or processed and, therefore, outside the storage devices, either before or after they are archived, the person in charge of them must safeguard them and prevent unauthorized persons from accessing them in any case.

Storage devices containing documents containing personal data classified as having a sensitive security level should be located in areas or premises where access is protected by access doors with key opening systems or other similar mechanisms. These areas must remain closed when access to such documents is not required. If it is not possible to comply with the above, the company BIO DIAGNOSTICOS S.A.S. may adopt duly motivated alternative measures that will be included in this document.

The description of the storage security measures can be found in numeral 6-7 of this document..

6. **Access to documents**.

Access to the documents must be made exclusively by the personnel authorized in numeral 12 of the manual, following the mechanisms and procedures defined. The latter must identify and preserve the access made to the classified documentation with a sensitive level of security, both by authorized users and by unauthorized persons as reflected in the aforementioned paragraph.

The procedure for accessing documents containing data classified as sensitive involves recording access to the documentation, the identity of the person accessing it, the time at which access occurs and the documents that have been accessed. Access to documents with this type of data is carried out by authorized personnel; if it is carried out by unauthorized persons, it must be supervised by an authorised user or by the security manager in question of the company BIO DIAGNOSTICOS S.A.S.

7. Security measures for automated databases.

7.1 Identification and authentication.

The company BIO DIAGNOSTICOS S.A.S., must install a computer security system that allows the users of the information systems to be correctly identified and authenticated, in order to guarantee that only authorized personnel can access the databases.

It must also establish a mechanism that allows the personalized and unambiguous identification of any user who tries to access the information system and that verifies whether he or she is authorized. Identification must be done by a unique system for each user accessing the information taking into account the username, employee ID, department name, etc. The nomenclature used for the assignment of usernames to access the information system and the authentication system of the users are included in numeral 12 of this document.

Where the authentication system is based on the entry of a password, a procedure for assigning, distributing and storing passwords must be implemented; To ensure the integrity and confidentiality of the latter, it is recommended that they be at least eight characters long and contain uppercase, lowercase, numbers, and letters. The password policy of the company BIO DIAGNOSTICOS S.A.S can be found in numeral 12 of this manual.

On the other hand, the company BIO DIAGNOSTICOS S.A.S must ensure that passwords are changed periodically, never for a period of more than 365 days. The period of validity of passwords is set out in the aforementioned numeral 12.

The company BIO DIAGNOSTICOS S.A.S, also guarantees the automated, internal and encrypted storage of passwords while they are valid, and will adopt a mechanism to limit repeated attempts at unauthorized access, also detailed in numeral 12 of the manual.

8. Entry and exit of documents or media

The entry of documents or media must be recorded indicating the type of document or medium, the date and time, the issuer, the number of documents or supports included in the shipment, the type of information they contain according to the level of security, the method of sending and the person responsible for receiving it. The departure or sending of documents or supports, duly authorised, must be recorded indicating the type of document or medium, the date and time, the recipient, the number of documents or supports included in the shipment, the type of information they contain according to the level of security, the method of sending and the person responsible for the shipment.

The entry and exit registration system must be attached to this document.

The facilities of the company BIO DIAGNOSTICOS S.A.S are the headquarters of the information systems that contain personal data must be duly protected in order to guarantee the integrity and confidentiality of said data; likewise, they must comply with the physical security measures corresponding to the document or medium where they include the data.

The company BIO DIAGNOSTICOS S.A.S. has the duty to inform its staff of its obligations in order to physically protect the documents or media in which the databases are located, not allowing their handling, use or identification by persons not authorised in this manual. The premises and facilities where the databases are located, specifying their physical characteristics and the existing physical security measures, are indicated in paragraph 12 of this document.

Only authorized personnel may have access to the places where the equipment that supports the information systems is installed, in accordance with the provisions of the aforementioned paragraph.

9. Data backup and recovery.

The company BIO DIAGNOSTICOS S.A.S. has carried out the necessary action procedures to make backup copies, at least once a week, except when there has been no update of the data during that period. All databases must have a backup from which data can be recovered.

Similarly, it has established procedures for the recovery of data with the aim of guaranteeing at all times that they are reconstructed to the state in which they were before their loss or destruction. When the loss or destruction affects partially automated databases, the data will be recorded manually, leaving a record of it in this manual.

The company BIO DIAGNOSTICOS S.A.S, will be in charge of controlling the correct operation and application of the procedures for making backup copies and recovery of data every 6 months.

The copying and backup procedures are set out in paragraph 12 of this manual.

The company BIO DIAGNOSTICOS S.A.S. must keep a backup copy of the data and its recovery procedures in a place other than the one where the equipment where its treatment is carried out is located. This place must in any case comply with the same security measures required for the original data.

10. Access log.

Attempts to access the information systems of the company BIO DIAGNOSTICOS S.A.S. must keep, at least, the identification of the user, the date and time in which it is carried out, the database accessed, the type of access and whether such access has been authorised or unauthorised. In the event that the registration has been authorised, the information that allows the identification of the consulted register is saved.

The security managers of the automated databases are responsible for controlling the mechanisms that allow access registration, reviewing the registered control information on a monthly basis and preparing a report of the reviews carried out and the problems detected. In addition, they must prevent the manipulation or deactivation of the mechanisms that allow access registration.

The data contained in the access log must be kept for at least two years.

Access registration will not be necessary when the data controller is a natural person and guarantees that only he or she has access to and processes the personal data. These circumstances must be expressly stated in this document.

Access to personal data through public or private communications networks must be subject to security measures equivalent to local access to personal data.

The transmission of personal data through public or wireless electronic communications networks must be carried out by encrypting said data, or using another similar mechanism that guarantees that the information is not intelligible or manipulated by third parties.

11. Functions and obligations of staff

All persons involved in the storage, processing, consultation or any other activity related to personal data and information systems must act in accordance with the functions and obligations set out in this section.

The company BIO DIAGNOSTICOS S.A.S, must inform its service personnel of the security measures and standards that correspond to the development of their functions, as well as the consequences of non-compliance, through any means of communication that guarantees their reception or dissemination (email, bulletin board, etc.). Likewise, you must make this Habeas Data Policies and Procedures manual available to staff so that they can learn about the security regulations and their obligations in this matter depending on the position they hold.

The company BIO DIAGNOSTICOS S.A.S, complies with the duty of information with its inclusion of confidentiality agreements and duty of secrecy subscribed, where appropriate, by the users of identification systems referred to in numeral 12 on databases and information systems, and by means of an informative circular addressed to them.

The functions and obligations of the staff of the company BIO DIAGNOSTICOS S.A.S are defined, in general, according to the type of activity they carry out within the institution, specifically, by the content of this manual. The list of users and profiles with access to protected resources is included in numeral 12 on databases and information systems. In general, when a user processes documents or media containing personal data, he or she has the duty to safeguard them, as well as to monitor and control that unauthorized persons cannot have access to them.

Failure to comply with the obligations and security measures established in this manual by the staff at the service of the company BIO DIAGNOSTICOS S.A.S is punishable in accordance with the regulations applicable to the legal relationship between the parties.

The functions and obligations of the users of the personal databases under the responsibility of the company BIO DIAGNOSTICOS S.A.S are the following:

Duty of secrecy: It applies to all persons who, in the course of their profession or work, access personal databases and links both users and contracted service providers; In compliance with this duty, the Organization's users may not communicate or disclose to third parties, data that they handle or of which they have knowledge in the performance or position of their functions, and must ensure the confidentiality and integrity of these.

Control functions and delegated authorizations: The data controller may delegate the processing of data to third parties, to act as a processor, by means of a data transmission contract. When data transmission contracts are signed, they will be annexed to this manual.

- The obligations related to the security measures implemented

- Access the databases only with due authorization and when necessary for the exercise of their functions.

- Do not disclose information to third parties or unauthorized users.

- Observe safety regulations and work to improve them.

- Do not carry out actions that pose a danger to the security of information.

- Do not take information from the organization's facilities without proper authorization.

- Use of resources and work materials: It must be oriented to the exercise of the assigned functions. The use of these resources and materials for personal purposes or unrelated to the tasks corresponding to the job is not authorised. When, for justified work reasons, it is necessary to remove peripheral or removable devices, it must be communicated to the security managers who may authorize it and, where appropriate, record it.

- Use of printers, scanners and other copying devices: When using this type of device, copies must be collected immediately, avoiding leaving them in their trays.

- Obligation to report incidents: Users are obliged to report incidents of which they are aware to those responsible for security, who will be responsible for their management and resolution. Some examples of incidents are: the failure of the computer security system that allows access to personal data to unauthorized persons, the unauthorized attempt to leave a document or medium, the perfidiousness of data or the total or partial destruction of media, the change of physical location of databases, the knowledge of passwords by third parties, the modification of data by unauthorized personnel, etc.

- Duty of custody of the media used: It obliges the authorised user to monitor and control that unauthorised persons access the information contained in the media. Supports containing databases must identify the type of information they contain by means of a labelling system and be inventoried. Where the information is classified with a sensitive security level, the labelling system should only be comprehensible to users authorised to access such informatio.

- Responsibility for work and laptop terminals: Each user is responsible for their own work terminal; when he/she is absent from his/her workstation, he/she must lock said terminal (e.g. screen saver with password) to prevent viewing or access to the information it contains; and has the duty to turn off the terminal at the end of the working day. Likewise, laptops must be controlled at all times to prevent their loss or theft.

Limited use of the Internet and e-mail: The sending of information electronically and the use of the Internet by the staff is limited to the performance of their activities within the company BIO DIAGNOSTICOS S.A.S.

- Safeguarding and protection of passwords: The passwords provided to users are personal and non-transferable, so their disclosure or communication to unauthorized persons is prohibited. When the user logs in for the first time with the assigned password, it is necessary to change it. When password reset is required, the user must notify the system administrator.

- Backup and recovery of data: All information from personal databases owned by the company BIO DIAGNOSTICOS S.A.S must be backed up.

- Duty to archive and manage documents and supports: Documents and supports must be duly archived with the security measures established in this chapter.

12. Databases and information systems.

The databases stored and processed by the company BIO DIAGNOSTICOS S.A.S are listed in the following table (Table I), which indicates the level of security and the treatment system of each of them.

Table I. Databases and security level

Database	Security Level
COLLABORATORS	High
SUPPLIERS	Basic
CLIENTS	Basic
PARTNERS	Basic

The following table (Table II) shows the structure of the databases of the company BIO DIAGNOSTICOS S.A.S.

Table II. Structure of the databases

Database Name	COLLABORATORS

Data controller	The company BIO DIAGNOSTICOS S.A.S **NIT**: 8000270721 **Address**: AV 6 A NORTE 20 N 53 BRR SANTA MONICA RESIDENCIAL **Telephone**: (602)6672320 **Email**: PROTECDATOS@BIODIAGNOSTICOS.CO
Queries and complaints manager	JULISSA VILLAMARIN VERGARA
Data type	Sensitive
Physical access control:	Authorized Users
Logical access control	Usernames and Passwords
Backups	Daily

Database Name	SUPPLIERS
Data controller	The company BIO DIAGNOSTICOS S.A.S NIT: 8000270721 **Address**: AV 6 A NORTE 20 N 53 BRR SANTA MONICA RESIDENCIAL **Telephone**: (602) 6672320 **Email**: PROTECDATOS@BIODIAGNOSTICOS.CO

Queries and complaints manager	JULISSA VILLAMARIN VERGARA
Data type	Basic
	Authorized Users
Logical access control	Usernames and Passwords
Backups	Daily

Database Name	CLIENTS
Data controller	The company BIO DIAGNOSTICOS S.A.S NIT: 8000270721 **Address**: AV 6 A NORTE 20 N 53 BRR SANTA MONICA RESIDENCIAL **Telephone**: (602)6672320 **Email**: PROTECDATOS@BIODIAGNOSTICOS.CO
Queries and complaints manager	JULISSA VILLAMARIN VERGARA
Data type	Basic
Physical access control:	Authorized Users
Logical access control	Usernames and Passwords
Backups	Daily

Database Name	**PARTNERS**
Data controller	The company BIO DIAGNOSTICOS S.A.S NIT: 8000270721 **Address**: AV 6 A NORTE 20 N 53 BRR SANTA MONICA RESIDENCIAL **Telephone**: (602)6672320 **Email**: PROTECDATOS@BIODIAGNOSTICOS.CO
Queries and complaints manager	JULISSA VILLAMARIN VERGARA
Data type	Basic
Physical access control:	Authorized Users
Logical access control	Usernames and Passwords
Backups	Daily

The appointment of the security officers does not relieve the controller or processor of their obligations.

The company BIO DIAGNOSTICOS S.A.S., identifies in this manual the data processors, as well as the conditions of the order. Where there is a data transfer contract, the processors are identified in the data transfer addendum to this document. Data processors must comply with the functions and obligations related to the security measures set out in this manual.

12.1 Procedure for reporting, managing and responding to incidents

The company BIO DIAGNOSTICOS S.A.S, establishes a procedure for notification, management and response to incidents in order to guarantee the confidentiality, availability and integrity of the information contained in the databases under its responsibility.

All users and those responsible for procedures, as well as any person who is related to the storage, processing or consultation of the databases contained in this document, must be aware of the procedure to act in the event of an incident.

The procedure for reporting, managing and responding to incidents is as follows:

When a person becomes aware of an incident that affects or may affect the confidentiality, availability and integrity of the institution's protected information, he or she must immediately notify the security officers, describing in detail the type of incident that occurred, and indicating the persons who may have been related to the incident, the date and time at which it occurred. the person who notifies the incident, the person to whom it is communicated and the effects it has produced.

Once the incident has been reported, you must request an acknowledgement of receipt from the corresponding security officer stating the notification of the incident with all the requirements listed above.

The company BIO DIAGNOSTICOS S.A.S, creates a record of incidents that must contain: the type of incident, date and time of the incident, person who notifies it, person to whom it is communicated, effects of the incident and corrective measures when applicable. This record is managed by the database security officer and should be included as an annex to this manual.

Likewise, it must implement the procedures for the recovery of the data, indicating who executes the process, the restored data and, if applicable, the data that has required to be manually recorded in the recovery process.

12.2 Report

All suspicious incidents and events should be reported as soon as possible through the internal channels established by the company BIO DIAGNOSTICOS S.A.S. If sensitive or confidential information is lost, disclosed to unauthorized personnel, or any of these events are suspected, the person responsible for the information must be notified immediately. Officials must report to their direct supervisor and/or to the Personal Data Protection Officer any damage or loss of computers or any other device, when they contain personal data in the possession of the Entity. Unless there is a duly reasoned and justified request from the competent authority, no official should disclose information about computer systems and networks that have been affected by a computer crime or abuse of a system. For the delivery of information or data by virtue of an order of authority, the Legal Advisory Office must intervene in order to provide appropriate advice.

The person responsible for the information must ensure that actions are taken to investigate and diagnose the causes that generated the incident, as well as guarantee that the entire incident management process is duly documented, supported by the Office of Technology and Information Technology.

13. ACCESS CONTROL AND VIDEO SURVEILLANCE

Access control: Areas where processes related to confidential or restricted information are carried out must have access controls that only allow authorized collaborators to enter and that allow the traceability of entries and exits to be maintained.

Video Surveillance: The Entity has video surveillance cameras that are intended to comply with physical security policies, complying with the parameters established in the Guide for the Protection of Personal Data in Video Surveillance Systems, issued by the SIC as the control authority. The images must be kept for a maximum time of 90 days. In the event that the respective image is the object or support of a claim, complaint, or any judicial process, until the moment it is resolved.

14. Measures for the transport, destruction and reuse of documents and media.

When it is necessary to discard any document (original, copy or reproduction) or medium containing personal data, it must be destroyed or deleted, through the implementation of measures aimed at preventing access to or recovery of the information contained in said document or medium.

Before starting the destruction, a record will be made or the record will be kept in a book or agenda, in said notation the document being destroyed will be described, the date, time and signature of the two people who evidence the destruction.

When the physical transfer of documents or media is carried out, they must adopt the necessary measures to prevent improper access, manipulation, theft or loss of information. The transfer of media containing personal data is carried out by encrypting the information, or using any other mechanism that guarantees that it is not manipulated or accessed.

The data contained in portable devices must be encrypted when they are outside the facilities that are under the control of the company BIO DIAGNOSTICOS S.A.S. Where encryption is not possible, the processing of personal data by means of such devices must be avoided; however, the treatment may be carried out when strictly necessary, adopting risk-taking safety measures and including them in this manual.

15. Violations and sanctions

In accordance with Chapter II of Statutory Law 1581 of 2012 on Data Protection, the Superintendence of Industry and Commerce may impose sanctions for non-compliance with data protection regulations on the data controller or the data processor. The possible sanctions are:

Fines of a personal and institutional nature up to the equivalent of two thousand (2,000) legal minimum monthly wages in force at the time of the imposition of the sanction. Fines may be successive as long as the non-compliance that gave rise to them persists.

Suspension of treatment-related activities for up to six (6) months. The act of suspension shall indicate the corrective measures to be adopted.

Temporary closure of operations related to the treatment once the suspension period has elapsed without the corrective measures ordered by the Superintendence of Industry and Commerce having been adopted.

Immediate and definitive closure of the operation involving the processing of sensitive data.

16. Validity

The databases under the responsibility of the company BIO DIAGNOSTICOS S.A.S. will be processed for as long as it is reasonable and necessary for the purpose for which the data are collected. Once the purpose or purposes of the processing have been fulfilled, and without prejudice to legal regulations that provide otherwise. The company BIO DIAGNOSTICOS S.A.S, will proceed to delete the personal data in its possession unless there is a legal or contractual obligation that requires its conservation. For all these reasons, this document enters into force on March 27, 2025.