REGULATION

ON COMMERCIAL SECRETS of BIOSINTEZ, PJSC

Penza, 2021

Table of Contents

1. GENERAL PROVISIONS

1.1. Purpose

This Regulation establishes the rules for establishing, changing and terminating the Confidential Information non-disclosure requirement to protect the confidentiality of this information.

1.2. Scope

This Regulation is binding on all Employees without exception.

The requirements of this Regulation also apply to Contractors to the extent established in the agreements between the Company and these Contractors and the Applicable Law.

2. TERMS AND DEFINITIONS

Unless otherwise expressly provided by the Regulations, the terms used herein have the following definitions:

(1) **Company** means BIOSINTEZ, PJSC that legally owns Confidential Information, has restricted access to this information and has established the non-disclosure requirement.

(2) **In-house policies and procedures** mean local regulations approved by the Company.

(3) **Regulation** means this Regulation on Commercial Secrets approved by the Company.

(4) **Commercial secrets** mean information non-disclosure requirement that allows increasing revenues, avoiding unjustified expenses, maintaining a position in the market of goods, works, services, or obtaining other commercial benefits by the Company under existing or possible conditions.

(5) **Confidential Information** means the information described in Section **Ошибка! Источник ссылки не найден.** hereof, in respect of which the Company has introduced the non-disclosure requirement.

(6) **Document** means a hard copy of the Confidential Information fixed on it.

(7) **Electronic Information** means Confidential Information provided electronically including:

- documents signed with digital signature;
- electronic images of the Documents of any format (scanned copy, photograph, image, etc.);
- information contained in the Corporate Programs of any format (databases, electronic files and documents, electronic correspondence, etc.).

(8) **Physical carrier** means floppy disks, optical discs, flash cards, hard drives, photo and video equipment and other physical carriers that contain Information in electronic form.

(9) **Corporate Equipment** means servers, computers, laptops, tablets, smartphones and other devices owned by the Company that contain Information in electronic form.

(10) **Corporate Programs** mean corporate mail, accounting programs, HR management programs, programs used for electronic document management and other computer programs developed and/or legally used by the Company and containing Information in electronic form.

(11) **IP-address** means a unique network address of a unit in a IP protocol-based computer network.

(12) **IP-address space** means the totality of all valid IP addresses of the Corporate Equipment that can be used to access them.

(13) **Employee** means an individual in an employment relationship with the Company of any position held, functions performed, place of work and other circumstances.

(14) **Head of the Company** means the Chief Executive Officer or other Officer of the Company authorized to perform all and/or part of the functions of the sole executive body in accordance with the Charter of the Company.

(15) **Officials of the Company** mean the Employees who are the heads of business units, departments and divisions of the Company and, within their official duties, make decisions on the disclosure and/or

provision of Confidential Information to Contractors, State Authorities and other third parties.

(16) **Contractor** means any Russian or foreign individual or legal entity to which the Company may disclose and/or transfer Confidential Information in any form.

(17) **State Authority** means a state authorities of the Russian Federation, state authorities of the Russian Federation, local government authorities, as well as authorities of the EAEU in accordance with the Applicable Law;

(18) **Classification code** means a warning label applied to Confidential Information (its carrier) in accordance with Section 8 of the Regulations to ensure its confidentiality.

(19) **Non-disclosure Commitment** means a written undertaking by an employee not to disclose the Company Confidential Information.

(20) **Applicable Law** means the regulations of the Russian Federation, constituent entities of the Russian Federation, local governments, as well as regulations of the EAEU authorities, international treaties in force on the territory of the Russian Federation.

(21) **RF** means the Russian Federation;

(22) **EAEU** means the Eurasian Economic Union.

3. CONCEPT OF CONFIDENTIAL INFORMATION

3.1. Information constituting the Commercial Secrets

The term **"Confidential Information"** means information of any nature that has actual or potential commercial value for the Company due to its secrecy to third parties, access to which is restricted for any third parties on a legal basis.

Confidential Information includes, in particular:

(1) production information;
(2) technical information;
(3) economic information;
(4) organizational information;
(5) information on the results of scientific and technical field intellectual activity;
(6) information of the professional activity method;
(7) any other information covered by the definition provided for in this Section.

The list of information classified by the Company as Confidential Information is provided in Appendix No. 1 to this Regulation.

3.2. Other confidential information

When performing its activities, the Company may receive, store and use other confidential information including:

(1) information received from third parties in respect of which the Company has assumed non-disclosure commitment;
(2) personal data of Employees and Contractors (individuals)
(3) other information that, in accordance with the Applicable Law, is not subject to disclosure (state secret, secret of the investigation, etc.).

With respect to the above confidential information, the same confidentiality measures are applied as specified in this Regulation with respect to Confidential Information, subject to the requirements of the Applicable Law and/or agreement with the third party that disclose this information to the Company.

4. NON-DISCLOSURE. RESTRICTION OF ACCESS TO THE CONFIDENTIAL INFORMATION

4.1. Non-disclosure introduction.

The Company establishes the non-disclosure requirement for all Confidential Information belonging to it.

The non-disclosure requirement provides for the introduction in the Company of legal, organizational and technical measures specified in this Regulation, required to protect Confidential Information.

The non-disclosure requirement applies to all Confidential Information on any type of carrier (form, place of its storage, other circumstances). The non-disclosure requirement applies equally to Confidential Information that:

(1) contained in all Documents without exception;

(2) presented as Information in electronic form and:

a. fixed on physical carriers (regardless of the owner of these physical carriers);

b. stored on the Corporate equipment (including equipment issued by the Company to the Employee);

c. available in the Corporate Programs (including those installed by the Company on the Employee's personal equipment).

(3) presented in a different way.

4.2. Restriction of Access to Confidential Information

The Company creates the required conditions for the protection of Confidential Information against unauthorized access and for the Employees to observe the non-disclosure requirement.

The measures implemented by the Company include:

(1) use of access control at the Company's premises, as well as video surveillance at the places where Confidential Information is stored;

(2) installation of locks on doors, placement of lockable cabinets, safes and boxes for the safe storage of Confidential Information in the premises of the Company;

(3) providing Employees with personal logins and passwords for access to the Corporate equipment and Corporate programs, including those installed by the Company on the Employee’s personal equipment;

(4) use of software measures to protect Confidential Information contained in the Corporate programs (anti-virus programs, information encryption, VPN connection, etc.);

(5) setting technical restrictions when using Corporate Equipment and Corporate Programs (blocking USB ports, limiting the size of files sent via the corporate mail, etc.);

(6) providing access to Confidential Information for Employees, disclosure of Confidential Information to Contractors and the State Authorities in accordance with the procedure and on the conditions provided for by the Regulation and the Applicable Law;

(7) registration of persons who have gained access to the Confidential Information (list of Employees who have received Corporate Equipment);

(8) marking Documents, Devices and Information in electronic form (when applicable) with a classification code in accordance with the Regulation.

(9) other measures provided for by this Regulation or the in-house policies and procedures.

As required, the Company has the right to take other measures aimed at protecting Confidential Information against unauthorized access that do not contradict the Applicable Law.

5. PROVISION OF ACCESS FOR EMPLOYEES TO THE CONFIDENTIAL INFORMATION

5.1. Disclosure of Confidential Information

The Company provides Employees with access to Confidential Information to the extent required for them to perform their job duties in accordance with the employment contract, job description and in-house policies and procedures.

To provide an Employee with access to Confidential Information, the Company shall:

(1) ensure the Employee reads and understands the Regulations against signature (including Appendix No. 1 thereto);

(2) obtain from the Employee a written non-disclosure commitment in the form provided in Appendix No. 2 to the Regulation.

Access to Confidential Information is provided to Employees depending on their position, division and other circumstances.

5.2. Termination of Access to Confidential Information

The Employee's access to Confidential Information is terminated in the following cases:

(1) at the initiative of the Head of the Company;

(2) at the initiative of the Company's Officer;

(3) in case of violation by the Employee of the confidentiality obligation stipulated by the Regulation, the Non-Disclosure Commitment, the Applicable Law;

(4) termination of the employment contract (for any reason).

Termination of access to Confidential Information is formalized by the relevant order of the Head of the Company with notification of this to the Employee against acknowledgment.

In case of termination of an employment contract (regardless of the reasons for termination), access to Confidential Information is terminated automatically and does not require an order from the Head of the Company.

Immediately after the termination of the Employee's access to Confidential Information, the Employee shall return to the Company all available Documents, physical carriers, their copies and derivative materials, as well as Corporate equipment, passes, keys to the storage of Confidential Information

6. HANDLING CONFIDENTIAL INFORMATION. NON-DISCLOSURE OBLIGATIONS OF EMPLOYEES

6.1. Confidentiality preservation

Employees shall observe the non-disclosure requirement for the Confidential Information and not disclose it to third parties.

Disclosure is an action or inaction, as a result of which the Confidential Information becomes known to third parties in any possible form (oral, written, other form, including using technical means) without the consent of the Company or contrary to an employment or civil law contract.

In particular, the following activities may be recognized as disclosure of Confidential Information prohibited by the Regulation:

(1) unauthorized oral disclosure of Confidential Information to third parties;

(2) unauthorized transfer of Documents, physical carriers, Corporate Equipment to third parties;

(3) unauthorized provision of the opportunity to copy, record, photograph, take notes or otherwise review the Confidential Information to third parties;

(4) forwarding (downloading) Confidential Information and information derived from it to personal mail;

(5) downloading and/or forwarding the specified information to himself/herself or third parties using other means of communication beyond the control of the Company (accounts in social networks, instant messengers, cloud storage, etc.);

(6) discussion of Confidential Information with third parties who do not have access to it, as well as in public places outside the Company's premises, in personal correspondence with third parties;

(7) unauthorized provision of access to the places of storage of Confidential Information (pass-cards, keys, passwords for gaining access to the Company's premises, to Corporate Equipment, Corporate Programs, etc.) to third parties;

(8) publication/mention of Confidential Information on the Internet (on websites, social networks, instant messengers), in the media (in print, on radio and television broadcasts), in public speeches, interviews and open correspondence.

Any disclosure of Confidential Information is prohibited and is recognized as a non-disclosure violation, for which liability is established by the Regulations and Applicable Law.

Employees undertake to take all possible and legal measures to prevent and suppress unauthorized access of third parties to Confidential Information, as well as actions of other Employees of the Company that may lead to the disclosure of Confidential Information.

6.2. Use of Confidential Information

Employees undertake to use Confidential Information for the purpose of their job duties and in the interests of the Company only.

The Employee is obliged not to disclose Confidential Information without the consent of the Company and not to use this information for personal purposes during the entire non-disclosure period, including after the termination of the employment contract.

When using Confidential Information, Employees undertake to:

(1) store Documents, physical carriers, Corporate equipment in the Company's premises, in lockable cabinets, safes, boxes;

(2) ensure the safety of the Corporate Equipment, physical carriers and Documents, which, according to the in-house policies and procedures, are allowed to be used outside the Company's premises;

(3) conduct all work correspondence only through the Company's corporate e-mail;

(4) apply on Documents, physical carriers, Information in electronic form (when applicable) the Classification in accordance with these Regulations;

(5) perform other duties stipulated by these Regulation and the non-disclosure obligation.

Employees are prohibited from:

(1) sending Information in electronic form to personal mail, messengers, social networks, cloud storage and other places outside the Company's information system;

(2) transferring the Corporate equipment, issued passes, keys and/or passwords to anyone;

(3) connecting personal peripherals to Corporate Equipment without permission;

(4) copying, outlining, photographing or otherwise recording Confidential Information for personal use, and/or unauthorized disclosure or transfer to third parties;

(5) taking any Documents, physical carriers out of the office of the Company without obtaining the permission of the Head of the Company or the Official;

(6) committing other acts that may lead to unauthorized disclosure of Confidential Information.

Making copies of documents containing Confidential Information is allowed in the scope required and sufficient for the purposes for which they are made, considering the requirements of the office workflow and document flow adopted by the Company.

Employees shall transfer Confidential Information to Contractors, as well as provide Confidential

Information to State Authorities in accordance with the requirements of this Regulation.

6.3. Company notification of non-disclosure violation

Employees shall immediately notify the Company:

(1) about any non-disclosure violations provided for by the Regulation by Employees, Contractors and/or State authorities;

(2) about the loss of Documents, physical carriers, Corporate Equipment, as well as personal equipment on which Corporate Programs are installed;

(3) about the loss of a pass card, access key to the Company's premises, login and password to the Corporate equipment and/or Corporate programs;

(4) on receipt (attempts to obtain) of unauthorized access to Confidential Information by third parties;

(5) other circumstances that entail or may entail a non-disclosure violation.

Notifications about the above events are sent by the Employee to the Official and/or the Head of the Company.

7. DISCLOSURE OF CONFIDENTIAL INFORMATION TO CONTRACTORS. DISCLOSURE OF CONFIDENTIAL INFORMATION TO STATE AUTHORITIES

7.1. Disclosure of Confidential Information to Contractors.

Disclosure of Confidential Information to Contractors is allowed only with the prior consent of the Head or Officer of the Company, subject to the requirements stipulated by the Regulation. Disclosure of Confidential Information to Contractors does not require prior consent if this disclosure is in accordance with the in-house policies and procedures approved by the Company. In this case, consent to the disclosure is considered received.

The employee who controls relations with the Contractor shall provide for the Contractor's non-disclosure obligations in writing.

To do this, before the disclosure of Confidential Information the Contractor shall conclude:

(1) Non-disclosure agreement; or

(2) A civil law contract containing the Contractor's non-disclosure obligations.

The above documents, concluded not in the form of the Company, are subject to approval by the Legal Department.

All Documents, physical carriers, Information in electronic form transferred and/or disclosed to the Contractors shall contain the Classification code in accordance with this Regulation.

7.2. Disclosure of Confidential Information to State Authorities

The Company shall disclose Confidential Information to the State Authorities in accordance with the procedure and under the terms provided for by the Applicable Law.

The grounds for the disclosure of Confidential Information to the State Authorities include:

(1) receipt by the Company of an official request from the State Authority on the need to disclose Confidential Information.

(2) receipt by the Company of state and municipal services and/or the passage of mandatory procedures provided for by the Applicable Law;

Confidential Information shall be disclosed to the State Authorities subject to a written consent of the Head or Officer of the Company. Disclosure of Confidential Information to State Authorities for the purpose of obtaining public services/passing through public procedures (registration of medicines, dietary supplements, registration of rights to the results of intellectual activity, filing documents with the court, etc.) does not require written consent.

Documents, physical carriers, information in electronic form, provided to the State Authorities, shall

contain the Classification code applied in accordance with this Regulation.

8. DESIGNATION OF PHYSICAL CARRIERS CONTAINING CONFIDENTIAL INFORMATION

8.1. Application of security classification label

Documents, physical carriers, information in electronic form transmitted to Contractors, State Authorities, other third parties, shall be marked with the “COMMERCIAL SECRET” Classification code indicating the name and location of the Company.

КОММЕРЧЕСКАЯ ТАЙНА
ПАО «БИОСИНТЕЗ»
г. Пенза, ул. Дружбы, д.4

COMMERCIAL SECRET
PJSC "BIOSINTEZ"
4, Druzhby Street, Penza, Russia

To apply this Regulation in the Company, the Classification codes “COMMERCIAL SECRET”, “CONFIDENTIAL INFORMATION” and “FOR OFFICIAL USE” are equivalent.

When fixing any information (including the creation of a Document, recording information on a physical carrier, creating Information in electronic form), the Employee, in agreement with the Official, shall determine whether this information is Confidential. When information is classified as Confidential, the Employee applies the Classification code to the Document, physical carrier or Information in electronic form (when applicable).

Classification code can be applied by the following methods:

(1) header or footer at the beginning or at the end of the page of electronic documents (when these documents are recorded on physical carriers, sent by e-mail, etc.);

(2) enclosing a cover letter to the Document and/or the physical carrier;

(3) as superimposed text ("watermarks") applied over the entire area of the page of the Document, Information in electronic form;

(4) as a stamp applied to the pages of the Document, a cover letter to the Document, physical carrier;

(5) as a sticker applied to the Documents and/or physical carrier;

(6) as text added to email

“This message and all attachments to it are strictly confidential and are intended solely for the use of the recipient (addressee). The information contained in this message is allowed to be used subject to the requirements of the legislation of the Russian Federation, the Regulation on Commercial Secrets of BIOSINTEZ, PJSC and non-disclosure agreements. If this message is received due to actions committed by accident or by mistake, the confidentiality of this information shall be observed. Do not use this information for any purpose. Please delete the received message without the possibility of recovery”;

(7) by other methods, not limited to those specified.

All correspondence coming from third parties with a Classification code applied or other similar designations (for example, “Company’s secret” etc.) is accepted and opened by the Employee who is entrusted with handling this information.

8.2. Declassifying

The Classification code from Documents, physical carriers, Information in electronic form shall be removed/canceled by the decision of the head of the Company on the proposal of the Official.

On Documents, physical carriers, cover letters, the Classification code is canceled by the Employee with a stamp or a handwritten note indicating the date of the non-disclosure cancellation. An analogue of the cancellation of the Classification code for Information in electronic form is the removal of the Classification code on the electronic documents themselves, indicating the date of the non-disclosure cancellation. An analogue of the cancellation of the Classification code for other physical carriers is the removal of the Classification code (stickers) from these physical carriers.

9. RESPONSIBLE PERSONS / DIVISIONS

The main obligations of the responsible persons/divisions are listed below:

(1) **Chief Executive Officer:**

- Approves the Regulation on Commercial Secrets;
- approves the disclosure/provision of Confidential Information to Contractors/State Authorities, as well as to other third parties;
- other actions provided for by the Regulation and the Applicable Law.

(2) **Officials of the Company:**

- supervise over the implementation of the Regulation by subordinate Employees;
- approve the disclosure/provision of Confidential Information to Contractors/State Authorities, as well as to other third parties;
- ensure obtaining of the Non-Disclosure Commitment from Employees;
- other actions provided for by the Regulation within their labor duties.

(3) **Human Resource department:**

- ensures newly hired Employees to read and understand the Regulation, including the list of Confidential Information against signature;

(4) **Information Technology Department:**

- issues Corporate equipment to Employees, as well as provides access to Corporate programs;
- keeps records of Employees who have received access to Confidential Information (who have received Corporate Equipment and access to Corporate Programs - logins, passwords);
- keeps records of Employees who has personal equipment with Corporate Programs installed;
- implements the means and methods of technical protection of Confidential Information approved by the Company.

(5) **Legal Department:**

- provides legal support and assistance when developing, amending the Regulation, as well as in its application;
- develops standard forms of legal documents provided for by the Regulation, as well as amends them;
- approves Non-disclosure Agreements provided by third parties;

10. COMPLIANCE CONTROL. OFFICIAL INVESTIGATIONS

If Confidential Information is disclosed, as well as other provisions of the Regulation are violated, the Company may conduct internal investigations.

The company shall conduct internal investigations by decision of the Head of the Company via a responsible person appointed (Employee or a third party).

If the violation is confirmed, the Employee may be subjected to measures provided for in Section 11 of this Regulation.

11. LIABILITY FOR NON-DISCLOSURE VIOLATION AND OTHER REQUIREMENTS OF THE REGULATION

11.1. Liability of Employees

For violation of the requirements of this Regulation, the Employee may be subject to disciplinary, civil, administrative and/or criminal liability.

The Company is entitled to take disciplinary actions against an Employee in case of violation by the Employee of the requirements of this Regulation. The Employee is brought to disciplinary responsibility in accordance with the Applicable Law and the in-house policies and procedures of the Company.

If the Employee's actions contain elements of an administrative offense and/or a crime, the Company is entitled to apply to law enforcement authorities to bring this Employee to administrative and/or criminal liability in accordance with the Applicable Law.

The Company is entitled to claim compensation by the Employee for losses caused by the disclosure of Confidential Information. A claim for damages may also be filed by the Company after the termination of the employment relationship with the Employee, if during the non-disclosure term this former Employee discloses Confidential Information that became known to him/her when performing his/her labor duties in the Company.

11.2. Liability of Contractors and State Authorities

The liability of Contractors and other third parties to the Company for non-disclosure violation in relation to Confidential Information is determined in accordance with the Applicable Law, considering the agreements concluded by the Company with the Contractors.

The liability of State Authorities and other third parties to the Company for non-disclosure violation is determined in accordance with the Applicable Law.

12. ENTRY INTO FORCE. AMENDING THE REGULATION

12.1. Entry into Force.

The Regulation shall enter into force in the Company from the date of its approval by order of the Head of the Company, unless otherwise provided by this order.

Non-disclosure Commitment obtained by the Company from Employees prior to the entry into force of this Regulation shall remain in force without renew and are applied subject to the requirements provided for in this Regulation.

The Classification codes applied to Documents, physical carriers, Information in electronic form and other physical carriers before the entry into force of this Regulation shall remain valid after the entry into force of the Regulation.

12.2. Amending the Regulation and other in-house policies and procedures

The Company may revise the Regulation and amend it when applicable, as well as in case of changes in the requirements of the Applicable Law.

Measures to ensure the establishment, change, cancellation of the non-disclosure requirement, as well as changes to the list of Confidential Information, shall be introduced by order of the Head of the Company. Employees shall read and understand the order against signature.

In case of changes to the in-house policies and procedures referred to in this Regulation, approval new in-house policies and procedures instead or in addition to them, Employees shall observe the new in-house

policies and procedures when performing their labor duties.

List of Appendices to the Regulation:

1. Appendix No. 1. List of Confidential Information of Biosintez, PJSC
2. Appendix No. 2. Non-disclosure obligation

ATTACHMENT No. 1.
To the Regulation on Commercial Secrets of BIOSINTEZ, PJSC

List of Confidential Information of BIOSINTEZ, PJSC

1. **Financial and economic information**
   - 1.1. Expected and actual indicators of financial and economic activities of BIOSINTEZ, PJSC (hereinafter referred to as the **"Company"**):
     - 1.1.1. details on the balance of income and expenditure of the Company;
     - 1.1.2. expected and actual indicators of profitability, profits, losses;
     - 1.1.3. financial transactions of the Company;
   - 1.2. Details of the state of the Company's bank accounts, cash flow and balances on the Company's accounts, transactions;
   - 1.3. Accounting registers;
   - 1.4. Primary accounting documents;
   - 1.5. Principles of operation and data of software and hardware accounting systems;
   - 1.6. Information relating to the tax and accounting policies of the Company;
   - 1.7. Loan sizes and terms;
   - 1.8. budget of the Company;
   - 1.9. Materials and results of internal and external audits and inspections of the Company;
   - 1.10. Information related to the financial transactions of the Company's contractors.
2. **Industrial-commercial and organizational information**
   - 2.1. Strategic development plans of the Company, prospects for its development; plans to expand the focus areas of the Company's activities in the market;
   - 2.2. Information about goals, objectives, programs, researches of the Company;
   - 2.3. Details of the conditions of the Company's experiments and the equipment on which they were conducted;
   - 2.4. Details of the features of the technologies used and developed and the specifics of their application; algorithms (formulas) of technological concepts applied and description of the principles of their work;
   - 2.5. Software developed by the Company and/or ordered by the Company, including source codes;
   - 2.6. Information that relates to the production secret (know-how) of the Company;
   - 2.7. Details of the features of the design and technological, art and technical designs of products that give a positive economic effect;
   - 2.8. Documents and information contained in registration dossiers for the Company's medicinal products, the results of clinical and/or post-registration studies of medicinal products, as well as information and documents regarding dietary supplements (except for information subject to disclosure in accordance with the law);
   - 2.9. Information about planned advertising campaigns;
   - 2.10. The content and resolution of internal meetings, as well as the content and resolution of negotiations with contractors;
   - 2.11. Management methods and forms of the Company, the procedure for making organizational and technical decisions and the technology for their implementation;
   - 2.12. Information on the preparation, adoption and execution of individual decisions of the

Company's management on commercial, organizational, production, scientific, technical and other issues;

2.13. Position, tactics and results of negotiation with third-party representatives (clients, partners, competitors);

2.14. Information about business partners, the nature and terms of relationships, financial results that are not provided in open sources;

2.15. Information constituting a commercial secret of partners, contractors of the Company and affiliated persons belonging to the same group of persons with the Company, disclosed as confidential;

2.16. Details of contractors, partners of the Company and affiliates that are members of the same group of persons with the Company and databases of contractors, partners and specified affiliates of the Company that are not provided in open sources;

2.17. Details of commercial and other terms of contracts between the Company and contractors;

2.18. Information, defined as confidential in accordance with the terms of civil law agreements, contracts, and agreements, under which the Company is one of the parties;

2.19. Details of the price calculation methods, the price level structure for products and the amount of discounts;

2.20. Results of research, analytical work, studies conducted in the interests of the Company, as well as information obtained during audits, provision of consulting services;

2.21. Information about the results of market research, containing assessments of the state and prospects for the development of market conditions;

2.22. The essence of the Company's position in court and arbitration cases;

2.23. Organizational structure of the Company.

2.24. Information constituting banking secrecy, information about the personal data of employees, partners and contractors of the Company that became known to an employee of the Company when performing his/her official duties and in accordance with the procedure established by the legislation of the Russian Federation.

3. Corporate Information

3.1. Details of the founders, participants of the Company, the structure of corporate governance of the Company, the procedure for making decisions in the Company, affiliated persons of the Company, if these details are not publicly available and not contained in the constituent documents of the Company, documents confirming keeping records about the Company in the relevant state register, in documents granting the right to perform business activities;

3.2. Meeting materials, minutes, decisions of the General Meeting of the Company's participants, the Board of Directors of the Company (except for those to be disclosed in accordance with the law).

4. Information and technical information and details related to security at the Company

4.1. Information about the composition, condition and location of software and hardware of the Company:

4.1.1. software algorithms;

4.1.2. passwords for entering the network, system, programs;

4.1.3. location of servers, archives and copies of credentials;

4.1.4. archiving method and procedure;

4.1.5. original software developments;

4.1.6. IP address space (internal, external);

4.2. Measures aimed at protecting the Company's local computer system against unauthorized access;

4.3. Equipment of communication, security and fire alarm networks and sets;

4.4. Details of the procedure and condition of the arrangement of security, access control, alarm system;

4.5. Other information of the procedure and status of the protection of information that constitutes the Company's Commercial Secret.

5. Other information

5.1. Any information that provides economic stability and advantage of the Company over competitors;

5.2. Logs, registers, registers of Documents, electronic Documents and other physical carriers of Confidential Information.

ATTACHMENT No. 2
To the Regulation on Commercial Secrets of BIOSINTEZ, PJSC

NON-DISCLOSURE COMMITMENT

Penza _____, 2021

I, [*Employee's full name*], employed in the position of [*position title*] hereinafter referred to as **the "Employee"**, give a written commitment (hereinafter referred to as **the "Commitment"**) as follows:

1. **Subject of the Commitment**
   1.1. I undertake not to disclose information constituting the Commercial secrets if it became known to me when performing my labor duties, and to observe the non-disclosure requirement established by the Employer.
   1.2. I realize that Commercial secrets mean information non-disclosure requirement, regardless of the type of carrier on which it is recorded, that allows increasing revenues, avoiding unjustified expenses, maintaining a position in the market of goods, works, services, or obtaining other commercial benefits by the Company under existing or possible conditions.
   1.3. I have read and understood the List of information constituting the Commercial secrets, as well as the measures for its protection specified in the Regulation on Commercial Secrets of BIOSINTEZ, PJSC.
   1.4. I undertake not to disclose information constituting the Commercial secrets during the entire non-disclosure period, including within 3 (three) years after the termination of the employment contract.
2. **Other obligations of the Employee**
   I undertake:

- observe the non-disclosure requirement in order to protect the confidentiality of information constituting the Commercial secrets;
- not to disclose information constituting the Commercial secrets if the Employer and its contractors are its owners, and not to use information for personal purposes without their consent;
- not to disclose confidential information obtained by accident or by mistake;
- upon termination of the employment contract, the Employee shall transfer to the Employer the physical carriers containing confidential information that were used by the Employee;
- not to disclose confidential information to family members, friends, as well as in social networks and other means of communication;
- not to make copies of physical carriers of confidential information;
- not to take physical carriers of confidential information outside the Employer's territory;
- not to use personal e-mail when working with confidential information;
- immediately inform the Employer about disclosure facts or the threat of disclosure of confidential information;
- observe the local regulations on Commercial secrets applied by the Employer.

3. **Liability of the Employee**
   In case of disclosure of confidential information, I am aware that the following liability measures may be applied to me: termination of the employment contract at the initiative of the Employer (item "c", cl. 6, part 1, article 81 of the Labor Code of the Russian Federation); bringing to full liability (cl. 7, part 1, article 243 of the Labor Code of the Russian Federation); administrative

responsibility according to Art. 13.14 of the Code of Administrative Offenses of the Russian Federation; criminal liability as per Art. 183 of the Criminal Code of the Russian Federation; compensation for losses of the Employer in case of disclosure of the Commercial secrets (during the non-disclosure term) after the termination of the employment relationship.

4. Final provisions

4.1. This Commitment is valid from the date of its signing.

4.2. Prior to signing this Commitment, I have read and understand:

- the List of information constituting the Commercial secrets;
- measures of liability for non-disclosure violation;

5. Details of the Employee

5.1. **Employee**: [*Full name*]

Position _____

EMPLOYEE'S SIGNATURE _____