Appendix 1

to the Bank of Russia Financial Messaging System Service Bureau Services Agreement

**RULES FOR THE PROVISION OF SERVICES OF THE BANK OF RUSSIA FINANCIAL MESSAGING SYSTEM SERVICE BUREAU**

Contents

[1. Terms and definitions 3](#_Toc124837228)

[2. General Provisions 4](#_Toc124837229)

[3. Entering into an Agreement 4](#_Toc124837230)

[4. Terms and conditions of service of the SPFS Service Bureau 4](#_Toc124837231)

[5. Terms and conditions for the right to use the Software 8](#_Toc124837232)

[6. Payment for Services 8](#_Toc124837233)

[7. Liability of the Parties 10](#_Toc124837234)

[8. Anti-corruption clause 11](#_Toc124837235)

[9. Personal data 11](#_Toc124837236)

[10. Confidentiality 12](#_Toc124837237)

[11. Term and Termination of the Agreement 12](#_Toc124837238)

[12. Dispute resolution procedure 12](#_Toc124837239)

[13. Miscellaneous 12](#_Toc124837240)

[Appendix 1 14](#_Toc124837241)

[Appendix 2 15](#_Toc124837242)

[Appendix 3 16](#_Toc124837243)

[Appendix 4 21](#_Toc124837244)

[Appendix 5 29](#_Toc124837245)

[Appendix 6 32](#_Toc124837246)

[Appendix 7 37](#_Toc124837247)

[Appendix 8 38](#_Toc124837248)

## Terms and definitions

* 1. "**Certificate of Readiness**" shall mean a Certificate of Readiness to Send Electronic Messages via the Service Bureau in the form set out in Appendix 2 to these Rules.
  2. "**IS Compliance Certificate**" shall mean a Certificate of Compliance by the Client with the Information Security Requirements in the form set out in Appendix 4 to these Rules.
  3. "**Details Form**" shall mean the Details Form of the User of the Financial Messaging System of the Bank of Russia in the form set out in Appendix 1 to these Rules.
  4. "**Agreement**" shall mean the Bank of Russia Financial Messaging System Service Bureau Services Agreement.
  5. "**EDI Agreement**" shall mean the Electronic Data Interchange Agreement.
  6. "**Service Request**" shall mean a request for services including providing advice, commenting on complaints, changing Software settings, preparing reports, providing information on supervisory requests and other services not related to Incident handling and specified in Appendix 8 to the Rules.
  7. "**Incident**" shall mean a complete or partial failure of the Software, as defined in Appendix 8 to the Rules.
  8. "**Client**" shall mean a legal entity that has entered into the Agreement with the Service Bureau.
  9. "**License Agreement**" shall mean the license agreement under which NSD grants a license to the licensee to use the Software.
  10. "**NSD**" shall mean National Settlement Depository.
  11. **Request** shall mean an enquiry for Incident handling services or fulfilment of a Service Request submitted by the Client to the Service Office by the means set out in Appendix 8 to the Rules.
  12. "**SPFS User**" shall mean a data interchange participant whose details are included in the List of SPFS Users.
  13. "**Rules**" shall mean these Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau, which are Appendix 1 to the Agreement.
  14. "**EDI Rules**" shall mean NSD's Electronic Data Interchange Rules.
  15. "**Software**" means Transit Terminal software owned exclusively by the Service Bureau.
  16. "**Service Bureau**" shall mean NSD as SPFS User, authorized by the agreement with the Bank of Russia to transmit third parties' financial information via the SPFS.
  17. "**SPFS**" shall mean the Financial Messaging System of the Bank of Russia.
  18. "**List of the Client's Authorized Representatives**" shall mean the List of the Client's Authorized Representatives which is Appendix 3 to the Agreement, in the form of Appendix 7 to the Rules.
  19. **NSD's Website** shall mean NSD’s official website at www.nsd.ru.
  20. "**List of SPFS Users**" shall mean the list that contains SPFS Users' details to be used to monitor the process of messaging via the SPFS.
  21. "**NSD's Fee Schedule**" shall mean the Fee Schedule for Services of the Bank of Russia Financial Messaging System Service Bureau.
  22. "**UID**" shall mean the unique identifier assigned to the message originator by the Bank of Russia.
  23. **Accounting Documents** shall mean primary accounting documents (invoices, statements on services rendered, as well as other documents stipulated by the legislation of the Russian Federation or the Agreement), tax accounting forms and documents if available (tax invoices and corrective tax invoices).
  24. Other terms shall have the meanings prescribed by the legislation of the Russian Federation, other regulations, regulations of the Bank of Russia, and the EDI Agreement.

## General Provisions

* 1. These Rules set out the methods and terms and conditions of providing Service Bureau's services.
  2. The Rules also set out the conditions under which the Service Bureau grants the Client the right to use the Software, where such right has not been granted to the Client on the basis of a separately concluded Licence Agreement. If there is the Licence Agreement, the terms and conditions of the Rules relating to the licensing of the Software shall not apply to the relationship between the Parties.

## Entering into an Agreement

* 1. The Service Bureau shall enter into an Agreement with those legal entities:
     1. with respect to which the Bank of Russia has given a notice that they may be included in the List of SPFS Users as Service Bureau clients;
     2. that have entered into an EDI Agreement with the Service Bureau;
     3. that have submitted the documents required by the [List of Documents to Be Submitted by Clients Being Legal Entities to NSD](https://www.nsd.ru/ru/documents/docs_in/), as available on NSD's Website. If a legal entity has already submitted a set of documents required by the List of Documents, the legal entity shall only submit those documents and/or amendments thereto which have not yet been provided.
  2. To enable the Bank of Russia to give notice that the legal entity may be included in the List of SPFS Users, the legal entity shall submit the following to NSD:
     1. the Details Form; and
     2. copies of any documents requested by the Bank of Russia.
  3. By submitting the Details Form to NSD, the legal entity shall be deemed to have confirmed that the details provided in the Details Form are accurate and may be included in the List of SPFS Users in case an Agreement is entered into.
  4. Within five (5) business days of the date of receipt of the complete set of documents referred to in Article 3.2of these Rules, NSD shall forward the information and documents received to the Bank of Russia for review. The time period during which those are to be reviewed shall be determined by the Bank of Russia.
  5. As soon as NSD receives a relevant notice from the Bank of Russia, NSD shall give notice to the legal entity's representative named in the Details Form.
  6. When NSD is notified of the legal entity admitted to the List of SPFS Users as Service Bureau client, the Parties shall commence negotiations with a view to enter into an EDI Agreement and an Agreement.

## Terms and conditions of service of the SPFS Service Bureau

* 1. The list of services provided by the Service Bureau includes:
     1. Connection to the SPFS;
     2. Providing the exchange of electronic messages between the Client and the SPFS Users.
  2. Connection to the SPFS consists in entering information about the Client into the List of SPFS Users maintained by the Bank of Russia.
  3. To enter the Client's details in the List of SPFS Users, the Service Bureau shall send to the Bank of Russia the information and documents specified in the agreement entered into between the Bank of Russia and the Service Bureau, upon receipt from the Client of the payment provided for in 6.3.1 of the Rules, if payment for such service is provided for by NSD's Tariffs. Otherwise, information and documents shall be sent to the Bank of Russia by the Service Bureau after the conclusion of the Agreement between the Parties.
  4. The deadline for entering the Client's information into the List of SPFS Users is determined by the Bank of Russia.
  5. Ensuring the exchange of electronic messages between the Client and the Users of the SPFS consists of the following activities on the part of the Service Bureau:
     1. receipt of Transit Electronic Document Packages from the Client;
     2. transmission of Electronic Messages contained in Transit Electronic Document Packages received from the Client to SPFS Users via the SPFS in accordance with the regulations of the Bank of Russia and the electronic messaging agreement between the Service Bureau and the Bank of Russia;
     3. receipt of Electronic Messages from the SPFS, the recipient of which is the Client;
     4. transmission of Electronic Messages from the SPFS to the Client in Transit Electronic Document Packages;
     5. maintaining archives of electronic messages sent/received through the SPFS;
     6. technical support, which consists of the following activities by the Service Bureau:
     7. informing the Client about the release of new versions of the Software;
     8. advising SPFS users when downloading Software updates;
     9. rectification of Incidents and servicing of Service Requests for the Software;
     10. providing advice on setting up the Software on the basis of the Client's requests;
     11. preparation of working instructions for SPFS Users in case the system is upgrated or updates are introduced.
  6. Technical support does not cover the following services:
     1. assembly, mounting (installation), setting up of key document production tools;
     2. repair of encryption (cryptographic) tools;
     3. repair, maintenance and servicing of information systems protected using encryption (cryptographic) tools;
     4. repair, maintenance and servicing of telecommunications systems protected using encryption (cryptographic) tools;
     5. repair, maintenance and servicing of key document production tools;
     6. IT infrastructure maintenance (servers, networking, PosgtreSQL, access rights, user accounts);
     7. advice or support to the client on how to organise a fail-safe solution.
  7. The exchange of electronic messages between the Client and the SPFS Users shall take place after confirmation of the Client's compliance with the Information Security Requirements, which are Appendix 3 to the Rules, and upon carrying out tests confirming that electronic communication between the Parties has been well established.
  8. Upon completion of the audit for compliance with the Information Security Requirements and the tests, the Parties shall execute a Certificate of Readiness (drawn up by the Parties) and an IS Compliance Certificate (drawn up by the Client). The Service Bureau shall ensure that the said certificates are retained for a period of five (5) years after their receipt from the Client.
  9. Afterwards, compliance with the Information Security Requirements shall be self-audited by the Client on an annual basis. The results of an audit shall be laid down in a Report on the Audit of Compliance with the Information Security Requirements in the Course of Message Interchange with the SPFS Service Bureau (Appendix 6 to these Rules), or in a Report on the Assessment of Compliance with the Information Protection Requirements in the SPFS Section in accordance with the National Standard of the Russian Federation GOST R 57580.2-2018 "Security of Financial (Banking) Transactions. Information Protection of Financial Organizations. Compliance Assessment Methodology", as approved by Order No. 156-st of the Federal Agency for Technical Regulation and Metrology dated 28 March 2018 "On the Approval of a National Standard of the Russian Federation" (M., FGUP "Standartinform", 2018).
  10. The Client shall be required to store information on the results of an annual self-audit for at least five (5) years and provide it to the Service Bureau upon request.
  11. The Service Bureau may audit the Client for compliance with the Information Security Requirements throughout the term of the Agreement by conducting desk audits or on-site audits.
  12. Transmission of Electronic Messages in the production environment:
      1. shall only be possible if the Client has been included in the List of SPFS Users, an UID has been assigned to the Client, the Parties have signed certificates referred to in Article 4.8 of these Rules, and the Client complies with these Rules;
      2. shall start no earlier than the date specified in the Certificate of Readiness;
      3. shall be carried out using the Software and NSD's File/Integration Gateway software. The granting of the right to use the Software is subject to the conditions set out in Section 5of the Rules or in a separate Licence Agreement concluded between the Parties. The right to use NSD's File/Integration Gateway software is granted subject to the terms and conditions of the license agreement available on NSD's website at <https://www.nsd.ru/documents/workflow/>
  13. Transit Electronic Document Packages that contain Electronic Messages to be transmitted via or that are received from the SPFS shall be interchanged by the Parties by way of Transit of electronic documents via the NSD EDI System in accordance with the EDI Agreement (Appendix 4 to the EDI Rules), subject to the provisions set out in Appendix 5 to these Rules.
  14. Confidentiality and immutability of Electronic Messages in a Transit Electronic Document Package shall be ensured by the Client by way of their encryption using the ESKVC of the SPFS User being the recipient.
  15. Specific requirements to the generation and/or interchange of Electronic Messages may be set out in operating and maintenance documentation provided by the Service Bureau.
  16. The Client shall:
      1. notify the Service Bureau of any impossibility to interchange (send and/or receive) Transit Electronic Document Packages/ Electronic Messages, as well as of any errors in the processing of Transit Electronic Document Packages/Electronic Messages, at the following e-mail addresses: [transit-help@nsd.ru](mailto:transit-help@nsd.ru) and [soed@nsd.ru](mailto:soed@nsd.ru);;
      2. notify the Service Bureau of any information security incidents at the following e-mail addresses: [soed@nsd.ru](mailto:soed@nsd.ru)and.[transit-help@nsd.ru](mailto:transit-help@nsd.ru). In case of such notification, authorized representatives of the Parties shall decide what steps are to be taken by the Parties to address and/or mitigate adverse consequences of the incident;
      3. appoint persons authorized to give notices referred to in Articles 4.16.2 and 4.16.2 above to the Service Bureau and provide the details of such persons to the Service Bureau in the List of the Client's Authorized Representatives at the same time when entering into the Agreement. In the event of replacement of authorized representatives and/or in the event of any changes in their details, the Client shall be obliged to provide the Service Bureau with an updated List of the Client's Authorized Representatives in the manner required by Article 13.2 of these Rules.
      4. ensure that the Transit Electronic Document Packages and their contents are generated, signed, encrypted, sent and received by authorised persons. Upon receipt of Transit Electronic Document Packages, the Service Bureau shall ensure that the signatory's authority is verified, with the contents of the Package being transferred to the recipient if it is signed either by the Client's sole executive body or by a person acting under a power of attorney containing the power of attorney form set out in the EDI Rules, authorising the signatory to sign and deliver any documents to the Service Bureau when providing the Client with the services, including Service Bureau services ("*for all other types of services provided by NSD*"). The Client shall independently arrange for the control of the amounts indicated in the transmitted Electronic Messages and the authority of the signatories;
      5. use up-to-date Software and NSD's File/Integration Gateway software;
      6. maintain the test and production segments (environments) and implement new versions (releases) of the Software on the production segment (environment) after testing them on the test segment (environment);
      7. monitor any Electronic Messages sent or received to ensure they do not contain a malicious code.
  17. The Client may suspend data interchange by sending a relevant application to the Service Bureau at the following e-mail addresses: [transit-help@nsd.ru](mailto:transit-help@nsd.ru)and[soed@nsd.ru](mailto:soed@nsd.ru).. The Service Bureau shall process the application and suspend data interchange with effect from the business day immediately next to the receipt of the application.
  18. The Service Bureau shall notify the Client of the occurrence/cessation of any circumstances that prevent data interchange by posting relevant information on NSD's Web Site. The Service Bureau shall take steps to ensure that data interchange is restored promptly.
  19. The Service Bureau may suspend services to the Client for a time period of any maintenance, tests, or other scheduled tasks. The Service Bureau shall notify the Client of the date and time of start and end of any such maintenance, tests, or other scheduled tasks at least two (2) business days before their commencement by posting relevant information on NSD's Web Site. Suspension of services as a result of any such maintenance, tests, or other scheduled tasks shall not be treated as service interruption.

## Terms and conditions for the right to use the Software

* 1. The right to use the Software is granted to the Client under a simple (non-exclusive) licence.
  2. The Software can be installed in the test and/or production environment of the Client an unlimited number of times.
  3. The right to use the Software is granted to the Client:
     1. for the duration of the Agreement, for use within the territory defined in the Agreement;
     2. for the purpose of information exchange between the Client and the Service Bureau when receiving services from the Service Bureau;
     3. The Client shall be entitled to use the Software in the manner set out in Article 1280.1 of the Civil Code of the Russian Federation.
  4. The Client shall not:
     1. transfer the right to use the Software to any third party:
     2. make changes to the code of the Software, except those made by the internal tools included in the Software and described in the operating and maintenance documentation;
     3. take any actions that lead to the removal or reduction of the effectiveness of the technical means of protection of the Software, including the use of software and hardware "multiplexing" means, means that modify the Software algorithm or hardware protection means, or use the Software with removed or modified protection means without the permission of the Rights Holder;
     4. reverse engineer, decompile and/or disassemble the Software, except and only to the extent that such activities are specifically permitted by applicable law.
  5. The Software shall be made available to the Client within five (5) working days from the date of payment of the invoice stipulated in paragraph 6.3.1 of the Rules and the invoice stipulated in paragraph 6.3.2 of the Rules by providing the Client with a link to download the Software at the e-mail address specified in the Agreement concluded between the Parties.

## Payment for Services

* 1. The Client shall pay for the services of the Service Bureau and pay the remuneration for the right to use the Software in the manner prescribed in the Rules and in the amount set forth in NSD's Fee Schedules.
  2. The fees and remuneration do not include value added tax (VAT), which shall be payable by the Client gross as established by Russian law. The fees and remuneration do not take into account taxes payable by the Client gross under the laws of other countries.
  3. The Service Bureau shall issue an invoice and provide other Accounting Documents in one of the ways specified in paragraph 6.4of the Rules, in the following order:
     1. The Service Bureau shall issue an invoice for the SPFS connection service within five (5) working days from the date the Agreement is concluded, if payment for such service is provided for by NSD's Fee Schedules. The Accounting Documents for the service shall be submitted by the Service Bureau no later than five (5) working days from the date of its provision.
     2. The Service Bureau shall invoice the Software Licence fee for the first full or partial calendar year of use of the Software within five (5) working days of entering into the Agreement. The Service Bureau shall provide the Accounting Documents upon granting the right to use the Software no later than five (5) working days from the date the Client is provided with the link to download the Software in accordance with paragraph 5.5 of the Rules;
     3. The Service Bureau shall issue an invoice for the electronic exchange service and submit other Accounting Documents at the latest on the fifth (5th) working day of the month following the billing month. The billing month shall be the calendar month in which the service is provided. The fee stipulated in this paragraph shall begin to be charged from the date of commencement of the exchange as specified in the Certificate of Readiness. In the case of an Agreement that provides for payment for the SPFS connection service, the Service Bureau shall start charging for the electronic messaging service either from the start date of the exchange as specified in the Certificate of Readiness or after 90 (ninety) days calculated from the date the Client connects to SPFS, whichever occurs first.
     4. The Service Bureau shall issue an invoice for the remuneration for the second and subsequent years of use of the Software and submit the other Accounting Documents by the fifth (5th) working day of January of the following year of use of the Software at the latest;
  4. Accounting Documents shall be made available to the Client:
     1. in the form of electronic documents via the Communication Channels provided for in the EDI Agreement and intended for the said purposes. The original hard copies of the Accounting Documents shall be made available at the Service Bureau's office. If necessary, the Service Bureau sends the originals of Accounting Documents to the postal address;
     2. in case the exchange of Accounting Documents has been enabled via an information system whose operator complies with the requirements of the Federal Tax Service of Russia, Accounting Documents are submitted in the manner prescribed by the EDI Agreement.
  5. In case of the exchange set out in paragraph 6.4.2 of the Rules has been enabled, the Parties shall follow the terms and conditions provided for in the EDI Agreement. In this case, other means of sending the Accounting Documents do not apply.
  6. The Client shall pay the invoice by wire transfer to the bank details of the Service Bureau specified in the invoice:
     1. in cases stipulated by clauses 6.3.1 and 6.3.2 of the Rules - within 10 (ten) business days from the date of sending the invoice in the form of an electronic document via the Communication Channels stipulated by the EDI Agreement;
     2. in the cases stipulated in clause 6.3.4 of the Rules - until 31 January.
     3. in the cases stipulated in clause 6.3.3 of the Regulation - not later than the 20th (twentieth) day of the month following the billing month.
  7. The date the invoice is paid is the date the funds is credited to the correspondent account of the Service Bureau.
  8. If the payment deadline is not met, the Service Bureau is entitled to demand payment of a penalty amounting to one (1) per cent of the overdue amount for each day of delay, but not exceeding ten (10) per cent of that amount.
  9. If payment is delayed for more than one calendar month, the Service Bureau can:
     1. suspend the provision of services;
     2. require payment by advance payment and not provide services if the advance payment made is not adequate.

## Liability of the Parties

* 1. The Parties shall be liable for failure to perform or improper performance of their obligations according to the legislation of the Russian Federation.
  2. The Service Bureau may not be held liable for failure to support electronic messaging between the Client and SPFS Users as a result of any disruption in the SPFS operation or violation by the Client of any requirements of these Rules.
  3. The Client shall be responsible for:
     1. for the content and ability to sign and send any Electronic Message it transmits through the Service Bureau, including the details of the recipient-users of the SPFS;
     2. ensuring compliance with the information security requirements set out in these Rules.
  4. If the Agreement is found to be non-existing or invalid due to either Party not having necessary authorizations or consents as may be required for that Party to enter into this Agreement, that Party shall indemnify the other Party against resulting losses.
  5. The Service Bureau shall not be liable for any damage resulting directly or indirectly from the use, misuse or inability to use the Software by the Client, loss of or damage to data. The Software is provided on an "as is" basis.
  6. The Service Bureau shall not be liable for the operation of the Software (and any losses caused) in the event that the Client (or third parties) have independently modified the Software or such failures are caused by incompatibility of the Software with other Client software or by a breach of the information security requirements set out in Appendix 3 to the Rules.
  7. The Parties shall be released from liability for non-performance or improper performance of its obligations under the Agreement if such non-performance or improper performance was caused by force majeure.
  8. A party that is unable to fulfil its obligations due to force majeure shall notify the other party of the occurrence/termination thereof.
  9. NSD shall be released from liability for non-performance or improper performance of its obligations under the Agreement if such non-performance or improper performance was caused by an emergency.
  10. An emergency may be defined as a situation involving the occurrence of circumstances that prevent Service Bureau from providing services to Clients and/or fulfilling its obligations to Clients, including:
      1. natural disasters (including earthquakes, floods, hurricanes);
      2. health and epidemiological circumstances (including mass diseases, epidemics and pandemics);
      3. circumstances of a technogenic nature (including complete or partial failure of communication networks, power supply systems, information systems and equipment beyond Service Bureau's control, as well as termination or restriction of access to information and telecommunication networks, including the Internet or its individual segments);
      4. acts of war, terrorist acts, sabotage, mass riots, strikes, political regime change, other political complications, both in the Russian Federation and in other states;
      5. decisions of public authorities, other bodies, institutions and organisations of the Russian Federation or other states; decisions of international organisations;
      6. fires or other accidents, destructions or significant damage to the premises occupied by the Service Bureau;
      7. any other circumstances which pose or may pose a threat to the life or health of employees of Service Bureau and/or Client.
  11. A situation is declared an emergency by the Service Bureau.
  12. The following decisions may be taken by the Service Bureau as measures to deal with the emergency and/or its consequences:
      1. change the manner, procedure and timeframe for providing services to the Client;
      2. any other actions to deal with the emergency and/or its consequences.
  13. When making decisions to deal with the consequences of emergencies, the Service Bureau may:
      1. set the time frame and procedure for implementing Service Bureau's decisions by the Client;
      2. condition the entry into force of Service Bureau's decisions on certain circumstances.
  14. The Service Bureau shall notify the Client of the measures taken to deal with the emergency and/or its consequences using available means of communication no later than the day on which such measures are taken.
  15. The Service Bureau and the Client shall act in the manner prescribed by the Service Bureau's decisions until the end of the emergency and/or its consequences.
  16. The Service Bureau shall take a decision to terminate the emergency and/or its consequences and shall notify the Client thereof.
  17. If the Service Bureau has reasonable doubts that the Client's representative is not authorised to sign electronic documents, the Service Bureau is entitled to suspend the exchange.

## Anti-corruption clause

* 1. The Parties shall, in accordance with the laws of the Russian Federation, develop and apply measures to prevent and counteract corruption. The Parties shall not engage in any activities qualifying under the laws of the Russian Federation as bribery and/or commercial bribery, shall not pay or offer to pay any money or value, directly or indirectly, to any persons to influence their actions or decisions in order to obtain any improper advantages or for any other improper purposes, and shall not take any other actions that violate the anti-corruption laws of the Russian Federation.

## Personal data

* 1. If either Party transfers any personal data to the other Party when entering into or performing the Agreement, it shall be mandatory that the transferring Party is authorized to transfer that personal data to the other Party, and the receiving Party shall be required to treat the personal data as confidential and process it in accordance with the principles and terms and conditions set out in the applicable laws of the Russian Federation. Upon receipt by either Party of a substantiated request from the other Party, the former Party shall be required to certify in writing the following within three (3) business days of the receipt of the request:
     1. its right to process personal data;
     2. its right to transfer personal data to the other Party (including certification that the data subject has been notified of the processing of his/her personal data); and
     3. its undertaking to keep that personal data confidential.

## Confidentiality

* 1. Neither Party may, without the other Party's prior written consent, disclose to third parties any information exchanged by the Parties in entering into the Agreement and/or information of which the Party became aware in the course of the Agreement performance, unless otherwise required by the laws of the Russian Federation and these Rules, and the Party shall take necessary measures required to safeguard that information.
  2. Either Party may disclose information exchanged by the Participants in connection with the entering into or performance of the Agreement to third parties engaged by that Party to perform its obligations under the Agreement, without the other Party's prior written consent. Confidential information may only be disclosed by a Party to a third party on terms and conditions similar to those set out in this section of these Rules.

## Term and Termination of the Agreement

* 1. The Agreement shall be deemed to take effect on the date of its signing and continue until, and inclusive of, 31 December of the year in which the Agreement is entered into. The Agreement shall be deemed to have been extended for each subsequent calendar year, unless a notice of non-renewal in writing is given by either Party to the other Party one (1) month prior to the end of the then current calendar year.
  2. The Agreement may be terminated either by mutual agreement between the Parties, or by either Party at its own discretion, without recourse to court.
  3. If the Agreement is terminated by either Party, the Agreement shall be deemed to have been terminated upon the expiry of ten (10) calendar days following the date when Service Bureau gives/receives the termination notice.
  4. A notice of non-renewal or a termination notice shall be either served to a representative of the other Party or mailed by registered letter to the other Party's postal address. The Service Bureau's postal address is available on NSD's Web Site.
  5. Termination of the Agreement shall not release the Parties from their respective obligations which arose before the termination date.

## Dispute resolution procedure

* 1. The Parties shall seek to resolve any and all disputes arising in the course of, or in connection, with the performance of the Agreement in accordance with the pre-trial complaint procedure. The Party with which a complaint is filed shall, within five (5) business days of the receipt of the original complaint, respond to it by either serving the response to a representative of the other Party or by mailing it by registered letter to the other Party's address recorded in the Unified State Register of Legal Entities (or, if the other Party is a non-resident of the Russian Federation, to its address available in another official source). If the Party fails to give a response to the complaint within the said time limits, the Party shall be deemed to have rejected the complaint.

## Miscellaneous

* 1. The law applicable to relations between the Parties shall be Russian law.
  2. Information letters or notices provided for by these Rules shall be sent by the Client from the e-mail addresses specified in the List of the Client's Authorized Representatives.
  3. Each Party shall be required to give notice to the other Party of any changes in the former Party's registered office address, postal address, or bank account details within three (3) business days of the effective date of such changes. The Service Bureau shall give notice of such changes to the Client by posting information on the changes on NSD's Web Site.

## Appendix 1

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

**Details Form of the User  
of the Financial Messaging System of the Bank of Russia**

|  |  |
| --- | --- |
| 1. **Organisation's details** | |
| Full company name |  |
| Short company name |  |
| Country of incorporation |  |
| Date of registration |  |
| SWIFT BIC |  |

|  |  |
| --- | --- |
| 1. **Details of the organization's accounts held with Russian banks** | |
| Availability of an account | *Yes/no* |
| Account type | *If any* |
| Details of the account bank | *If any* |
|  |  |
| 1. **Contact details of the representative** | |
| Name, surname |  |
| Job title |  |
| Email |  |
| Telephone number |  |

|  |  |
| --- | --- |
| 1. **Other details** | |
| Preferred language for communication |  |

*By signing this Details Form, I give my consent to NSD (Principal State Registration Number (OGRN) 1027739132563) to process my personal data contained herein and confirm that I have the right to give consent to NSD to process the personal data contained herein, including its transfer to the Central Bank of the Russian Federation, for the purpose of receiving a notice that the organization may be included in the list of users of the Financial Messaging System of the Bank of Russia as service bureau client.*

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Job title)* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Signed)* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Name, surname)* |

## Appendix 2

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

SAMPLE FORM

**Certificate of Readiness  
to Send Electronic Messages via the Service Bureau**

Moscow \_\_\_\_ \_\_\_\_\_\_\_20\_\_

This Certificate of Readiness to Send Electronic Messages via the Service Bureau is executed by National Settlement Depository (the "Service Bureau") represented by \_\_\_\_\_\_\_\_\_\_\_ acting under \_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the "Client") represented by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ acting under \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (together, the "Parties" and individually, a "Party") to certify as follows:

1. The software provided to the Client the purposes of interchanging electronic messages via the Service Bureau has been installed.
2. The Parties have conducted tests that showed the possibility to start interchanging Transit Electronic Document Packages / Electronic Messages in the production environment.
3. Data interchange in the production environment may be commenced by the Parties with effect from \_\_ \_\_\_\_\_\_\_\_\_ \_\_\_\_.
4. This Certificate is made in two (2) originals of equal validity, one original for each of the Parties.

|  |  |
| --- | --- |
| **Service Bureau** | **Client** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| L.S. | L.S. |

## Appendix 3

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

|  |  |  |
| --- | --- | --- |
| **No.** | **Information Security Requirements** | |
| **1.** | The information infrastructure components used for the purpose of sending electronic messages are installed by the Client in dedicated (standalone) segments (groups of segments) of computer networks ("information infrastructure components"). | |
| With respect to information infrastructure components within the said segment (groups of segments) of computer networks, the Client applies the following information security controls[[1]](#footnote-2): | |
| **1.1** | information protection in the course of access management | arrangement and control of the use of logical access subjects' user accounts; |
| arrangement and control of granting (revocation) and blocking of logical access; |
| logging of information security events relating to the use of user accounts and logical access rights, and logical access control; |
| identification and authentication of logical access subjects; |
| control and protection of identification and authentication data; |
| authorization (access control) for logical access purposes; |
| logging of information security events relating to identification, authentication or authorization for logical access purposes; |
| arrangement and control of physical access to rooms in which information infrastructure components are installed; |
| logging of information security events relating to physical access; |
| documentation and control of information infrastructure resources and components; |
| logging of information security events relating to changes in information infrastructure resources and components. |
| **1.2** | ensuring the protection of computer networks | segmentation and firewalling of local area networks; |
| protection of local area networks in the course of interaction with the Internet; |
| logging of information security events relating to changes in LAN security parameters; |
| monitoring and control of network traffic content; |
| logging of information security events relating to monitoring and control of network traffic content; |
| information protection against disclosure and modification when using wireless networks; |
| protection of local area networks when using wireless networks; |
| logging of information security events relating to the use of wireless networks. |
| **1.3.** | integrity and security control of information infrastructure | control to make sure information infrastructure components are not affected by known (described) information security vulnerabilities; |
| arrangement and control of the processes of hosting, storage and update of information infrastructure software; |
| composition and integrity control of information infrastructure software; |
| logging of information security events relating to integrity and security control of information infrastructure. |
| **1.4.** | protection against a malicious code | defence-in-depth to protect against a malicious code at different levels of information infrastructure; |
| arrangement and control of the application of tools designed for protection against a malicious code; |
| logging of information security events relating to protection against a malicious code. |
| **1.5.** | prevention of data leakage | blocking of forbidden (and control of permitted) potential channels of data leakage; |
| control (analysis) of information transmitted via permitted potential channels of data leakage; |
| protection of machine-readable media; |
| logging of information security events relating to data leakage prevention. |
| **1.6.** | information security incident management | monitoring of data concerning logged information security events, which is generated by information protection tools and systems and by information infrastructure components; |
| collection, protection and storage of data concerning logged information security events; |
| analysis of data concerning logged information security events; |
| logging of information security events relating to the processing of data concerning logged information security events; |
| detection and logging of information security incidents; |
| responding to information security incidents; |
| storage and protection of information on information security incidents; |
| logging of information security events relating to detection of and responses to information security incidents. |
| **1.7.** | virtualization environment protection | identification, authentication and authorization (access control) for logical access purposes; |
| segmentation and firewalling of computer networks |
| **1.8.** | information protection in case of remote logical access using mobile (portable) devices. | |
| **2.** | Documents prepared by the Service Bureau's Client to ensure information protection when sending electronic messages shall set out the following details: | processes of preparation, processing, transmission, and storage of electronic messages and protected information using information infrastructure; |
| a list and rules of usage of information protection tools applied to control the integrity of and authenticate electronic messages at the stages of their generation (preparation), processing, transmission, and storage, including methods of using data encryption tools and managing data encryption tools' key information; |
| a plan of actions to ensure continuity and/or disaster recovery of processes relating to electronic message interchange; |
| persons authorized to use data encryption tools; |
| persons responsible for ensuring the functioning and security of data encryption tools (responsible data encryption tool users); |
| persons authorized to control cryptographic keys, including those responsible for generation of cryptographic keys and ensuring their security; |
| persons authorized to report information security incidents detected during electronic message interchange. |
| **3.** | The details of persons authorized to report information security incidents detected during electronic message interchange shall be provided by the Client to the Service Bureau no later than the next day following their appointment or replacement. | |
| **4.** | Sending and receiving electronic messages between the Service Bureau and the Client shall be maintained using a workstation designed for electronic message interchange. | |
| **5.** | The Client shall store incoming and outgoing electronic messages for at least five years of their receipt/sending. | |
| **6.** | Protection of electronic messages during their transmission to the Service Bureau by way of generating electronic messages and controlling their attributes in the information infrastructure shall be ensured by the Client in accordance with the following requirements: | |
| **6.1.** | The segment in which electronic messages are generated and the segment in which their attributes are controlled in the Client's information infrastructure shall be segregated, with different workstations and different employees being used in each of the segments. | |
| **6.2.** | The Client's information infrastructure components used in the segment in which electronic messages are generated and those used in the segment in which electronic message attributes are controlled shall be installed in different computer network segments, including virtual segments. The process of permitted interaction between the said computer network segments shall be duly documented and approved by the Client's information security function. | |
| **6.3.** | In the segment in which electronic messages are generated, the following steps shall be taken either on the basis of an underlying document in hard copy or electronic format, or on the basis of an incoming electronic message: | generation of an outgoing electronic message to be sent to the Service Bureau; |
| controlling the attributes of the outgoing electronic message to be sent to the Service Bureau; |
| signing the outgoing electronic message to be sent to the Service Bureau, using for that purpose an electronic signature intended to be used in the segment in which electronic messages are generated, provided that the control of the electronic message attributes has returned positive results; |
| sending the outgoing electronic message to be sent to the Service Bureau to the segment in which electronic message attributes are controlled. |
| **6.4.** | In the segment in which electronic message attributes are controlled, the following steps shall be taken: | controlling the attributes of the outgoing electronic message to be sent to the Service Bureau to make sure those match the details of the underlying document in hard copy or electronic format or the incoming electronic message; |
| controlling duplicate outgoing electronic messages; |
| provided that the control of the electronic message attributes has returned positive results, sending the outgoing electronic message to the workstation designed for electronic message interchange, with further encryption of the electronic message at the application layer using the seven-layer basic model of open systems interconnection, as described in ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. Open Systems Interconnection. Basic Reference Model. The Basic Model. |
| **7.** | When interchanging electronic messages with the Service Bureau, electronic messages shall be protected in accordance with the following requirements: | |
| **7.1.** | Data protection tools shall be used which ensure mutual authentication and data encryption at the session layer (layer 5) and below layers, in accordance with the basic model of open systems interconnection, as described in ISO/IEC 7498-1:1994 Information technology.  Open Systems Interconnection. Basic Reference Model. The Basic Model. | |
| **7.2.** | In interacting with the Service Bureau, it is recommended to use hardware that have pre-approved unique remotely identifiable identification characteristics (IP address, DNS, etc.) and to prohibit connecting any hardware with different identification characteristics. | |
| **8.** | For the purposes of analysis of measures applied to protect information in the course of data interchange, the Client (a Client's authorized person) shall notify the Service Bureau of any information security incidents detected during the electronic message interchange within eight business hours of the incident detection, by sending an information message by any method available. | |

## Appendix 4

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

SAMPLE FORM

**Certificate of Compliance  
by the Client with the Information Security Requirements**

|  |  |  |
| --- | --- | --- |
|  | APPROVED | |
|  | *(Job title)* | |
|  | *(Signed)* | *(Name, surname)* |
| L.S. | |
|  | \_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ | |

This Certificate is executed following the audit of readiness to interchange electronic messages using NSD File/Integration Gateway and Terminal Transit software

The Commission of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*Client's name*) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ established by Order No.\_\_\_ dated \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, comprised of:

|  |  |  |
| --- | --- | --- |
|  | Commission chairperson: |  |
|  | Commission members: |  |
|  |  |  |
|  |  |  |
|  |  |  |

has audited the Client's readiness to interchange electronic messages with the SPFS Service Bureau

and found the following:

1. The location and technical condition of the hardware, systems, and network and telecommunications equipment, as well as the condition of the workstation software, meet the recommendations issued by the SPFS Service Bureau, namely:
   1. The hardware, systems, and network and telecommunications equipment of the workstations designed for data interchange are installed in the following rooms: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ at the following address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which meet the security requirements (i.e., the rooms are equipped with an intrusion detection and alarm system, guarded, and covered by a CCTV and access control system), and are in good repair and ready for operation.
   2. The necessary software designed to support electronic data interchange, including security tools designed to protect against malicious codes \_\_\_\_\_\_\_\_\_\_, and data encryption tools Validata are installed on the workstations designed for data interchange and set up in accordance with the applicable instruction manuals.
   3. Redundant software and hardware are available and ready to use.
   4. Communications with the SPFS Service Bureau via \_\_\_\_\_\_\_\_\_ are supported by the following telecommunications providers: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (primary channel) and \_\_\_\_\_\_\_\_\_\_\_ (backup channel).
2. The following method of interaction between the Client's IT systems and the workstations designed for data interchange is used: file.
3. Information security during electronic message interchange is maintained in accordance with the following requirements:
   1. The information infrastructure components used by the Service Bureau's Client for the purpose of sending electronic messages are installed in dedicated (standalone) segments (groups of segments) of computer networks ("information infrastructure components").
   2. With respect to information infrastructure components within the said segment (groups of segments) of computer networks, the Service Bureau's Client applies the following information protection measures in accordance with the National Standard of the Russian Federation GOST R 57580.1-2017 "Security of Financial (Banking) Operations. Information Protection of Financial Organizations. Basic Set of Organizational and Technical Measures", as approved by Order No. 822-st of the Federal Agency for Technical Regulation and Metrology dated 8 August 2017 "On the Approval of a National Standard of the Russian Federation" (M., FGUP "Standartinform", 2017):

* information protection in the course of access management;
* ensuring the protection of computer networks;
* integrity and security control of information infrastructure;
* protection against a malicious code;
* prevention of data leakage;
* information security incident management;
* virtualization environment protection[[2]](#footnote-3);
* information protection in case of remote logical access using mobile (portable) devices[[3]](#footnote-4).
  1. The following technologies are not used by the Client in the specified segment(s) of the computer network:
* *List the technologies that are not used in the electronic document transmission segment, e.g. virtualisation technology, wireless network technology, technology for remote access to infrastructure objects from mobile hand-held devices.*
  1. The following information security measures have been implemented by the Service Bureau in terms of ensuring the protection of information when managing the Client's access:
* arrangement and control of the use of logical access subjects' user accounts;
* arrangement and control of granting (revocation) and blocking of logical access;
* logging of information security events relating to the use of user accounts and logical access rights, and logical access control;
* identification and authentication of logical access subjects;
* control and protection of identification and authentication data;
* authorization (access control) for logical access purposes;
* logging of information security events relating to identification, authentication or authorization for logical access purposes;
* arrangement and control of physical access to rooms in which information infrastructure components are installed;
* logging of information security events relating to physical access;
* documentation and control of information infrastructure resources and components;
* logging of information security events relating to changes in information infrastructure resources and components.
  1. The following information security measures have been implemented by the Service Bureau to ensure the protection of computer networks:
* segmentation and firewalling of local area networks;
* protection of local area networks in the course of interaction with the Internet;
* logging of information security events relating to changes in LAN security parameters;
* monitoring and control of network traffic content;
* logging of information security events relating to monitoring and control of network traffic content;
* information protection against disclosure and modification when using wireless networks[[4]](#footnote-5);
* protection of local area networks when using wireless networks[[5]](#footnote-6);
* logging of information security events relating to the use of wireless networks[[6]](#footnote-7).
  1. To monitor the integrity and security of the information infrastructure, the Client has implemented the following information security measures:
* control to make sure information infrastructure components are not affected by known (described) information security vulnerabilities;
* arrangement and control of the processes of hosting, storage and update of information infrastructure software;
* composition and integrity control of information infrastructure software;
* logging of information security events relating to integrity and security control of information infrastructure.
  1. To protect against malicious code, the Client has implemented the following information security measures:
* defence-in-depth to protect against a malicious code at different levels of information infrastructure;
* arrangement and control of the application of tools designed for protection against a malicious code;
* logging of information security events relating to protection against a malicious code.
  1. To prevent information leaks, the Client has implemented the following information security measures:
* blocking of forbidden (and control of permitted) potential channels of data leakage;
* control (analysis) of information transmitted via permitted potential channels of data leakage;
* protection of machine-readable media;
* logging of information security events relating to data leakage prevention.
  1. In terms of information security incident management, the Client has implemented the following information security measures:
* monitoring of data concerning logged information security events, which is generated by information protection tools and systems and by information infrastructure components;
* collection, protection and storage of data concerning logged information security events;
* analysis of data concerning logged information security events;
* logging of information security events relating to the processing of data concerning logged information security events;
* detection and logging of information security incidents;
* responding to information security incidents;
* storage and protection of information on information security incidents;
* logging of information security events relating to detection of and responses to information security incidents.
  1. To protect the virtualisation environment, the Client has implemented the following information security measures[[7]](#footnote-8):
* identification, authentication and authorization (access control) for logical access purposes;
* segmentation and firewalling of computer networks;
* organisation of identification, authentication, authorisation (access delimitation) when logical access to virtual machines and server components of virtualisation is performed;
* organising and controlling the communication and isolation of virtual machines;
* organisation of virtual machine image protection;
* registration of information security events related to access to virtual machines and server components of virtualisation.
  1. With regard to information protection when performing remote logical access using mobile (portable) devices, the following information protection measures have been implemented by the Client[[8]](#footnote-9):
* Protection of information from disclosure and modification by remote access;
* protection of internal computer networks in the case of remote access;
* protection of information from disclosure and modification during its processing and storage on mobile (portable) devices.
  1. The provisions of the international standard ISO/IEC 27002:2013 Information technology. Security techniques. Codes of practice for information security controls. shall/shall not apply to the implementation of information security requirements by the Client of the Service Bureau.

1. The Client has drawn up documents defining the procedure for ensuring the protection of information during the transmission of electronic messages:

* technologies for the preparation, processing, transmission and storage of electronic messages and protected information at information infrastructure facilities are defined in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* a list and rules of usage of information protection tools applied to control the integrity of and authenticate electronic messages at the stages of their generation (preparation), processing, transmission, and storage, including methods of using data encryption tools and managing data encryption tools' key information are defined in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* a plan of actions to ensure continuity and/or disaster recovery of processes relating to electronic messaging is set out in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. The Client of the Service Bureau has ensured the protection of the electronic messages created when transmitting them to the Service Bureau by generating electronic messages and controlling the details of electronic messages in the information infrastructure, taking into account the following:
   1. The segment in which electronic messages are generated and the segment in which their attributes are controlled in the Client's information infrastructure shall be segregated, with different workstations and different employees being used in each of the segments.
   2. The Client's information infrastructure components used in the segment in which electronic messages are generated and those used in the segment in which electronic message attributes are controlled shall be installed in different computer network segments, including virtual segments. The process of permitted interaction between the said computer network segments has been duly documented and approved by the Client's information security function.
   3. In the segment in which electronic messages are generated, the following steps shall be taken either on the basis of an underlying document in hard copy or electronic format, or on the basis of an incoming electronic message:

* generation of an outgoing electronic message to be sent to the Service Bureau;
* controlling the attributes of the outgoing electronic message to be sent to the Service Bureau;
* signing the outgoing electronic message to be sent to the Service Bureau, using for that purpose an electronic signature intended to be used in the segment in which electronic messages are generated, provided that the control of the electronic message attributes has returned positive results;
* sending the outgoing electronic message to be sent to the Service Bureau to the segment in which electronic message attributes are controlled.
  1. In the segment in which electronic message attributes are controlled, the following steps shall be taken:
* controlling the attributes of the outgoing electronic message to be sent to the Service Bureau to make sure those match the details of the underlying document in hard copy or electronic format or the incoming electronic message;
* controlling duplicate outgoing electronic messages;
* provided that the control of the electronic message attributes has returned positive results, sending the outgoing electronic message to the workstation designed for electronic message interchange, with further encryption of the electronic message at the application layer using the seven-layer basic model of open systems interconnection, as described in ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. Open Systems Interconnection. Basic Reference Model. The Basic Model;

1. The Client has ensured that, when interchanging electronic messages with the Service Bureau, electronic messages are protected in accordance with the following requirements:
   1. Data protection tools shall be used which ensure mutual authentication and data encryption at the session layer (layer 5) and below layers, in accordance with the basic model of open systems interconnection, as described in ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model.
   2. In interacting with the Service Bureau, steps are / are not taken to ensure the use of hardware that have the following pre-approved unique remotely identifiable identification characteristics: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (IP address, DNS, etc.) \_\_\_\_\_\_\_\_\_, and connecting any hardware with different identification characteristics is prohibited.
2. The testing was conducted successfully using \_\_\_\_\_\_\_\_\_\_\_\_ during the period from \_\_\_\_\_\_\_\_ to \_\_\_\_\_\_\_\_\_.
3. The following responsible persons are appointed (their roles may overlap):
   1. persons authorized to use data encryption tools:

|  |  |  |  |
| --- | --- | --- | --- |
| Name, surname | Job title | Telephone | Appointment document details |
|  |  |  |  |

* 1. persons responsible for ensuring the functioning and security of data encryption tools:

|  |  |  |  |
| --- | --- | --- | --- |
| Name, surname | Job title | Telephone | Appointment document details |
|  |  |  |  |

* 1. persons authorized to control cryptographic keys, including those responsible for generation of cryptographic keys and ensuring their:

|  |  |  |  |
| --- | --- | --- | --- |
| Name, surname | Job title | Telephone | Appointment document details |
|  |  |  |  |

* 1. persons authorised to report detected incidents involving breaches of information security requirements in financial messaging:

|  |  |  |  |
| --- | --- | --- | --- |
| Name, surname | Job title | Telephone | Appointment document details |
|  |  |  |  |

**Opinion**

The Commission believes that \_\_\_\_\_\_\_\_\_\_\_\_\_ (Client's name) \_\_\_\_\_\_\_\_ is ready to interchange electronic messages with the SPFS Service Bureau for money transfer purposes.

|  |  |
| --- | --- |
| Commission chairperson: |  |
| Commission members: |  |
|  |  |
|  |  |

Appendices: Notices of the appointment of persons listed in paragraph 8 of the Certificate.

## Appendix 5

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

**Specific Aspects of the Process of Interchanging Transit Electronic Document Packages**

1. **Specific Aspects of Application of Appendix 4 to the EDI Rules to Electronic Message Interchange between the Parties**
   1. The rules of Transit of electronic documents via the NSD EDI System shall apply to Electronic Message interchange between the Client and the Service Bureau to the extent to which those rules relate to:
      1. generation and sending of Transit Electronic Documents; and
      2. processing of Transit Electronic Document Packages.
2. **Generation and Sending of Transit Electronic Document Packages by the Client**
   1. To generate Electronic Messages, as well as to send and receive Transit Electronic Document Packages, a Client that is a credit institution shall use the Software.
   2. Electronic Messages to be sent to the Service Bureau shall be generated using applicable electronic message formats in accordance with the Album of Unified Formats of Electronic Banking Messages "Unified Formats of Electronic Banking Messages for Wireless Payments. Data Interchange with Credit Institutions and Other Customers of the Bank of Russia in the Context of Interaction between Users of the Bank of Russia Financial Messaging System” posted on the Internet at [www.cbr.ru.](http://www.cbr.ru))
   3. The description of a Transit Electronic Document Package (winf.xml) the specifications of which are set out in Appendix 3 to the EDI Rules shall be prepared in accordance with the following specific provisions:
      1. formal description (DTD):

<!ELEMENT COVERING\_LE

TTER (ORIGINATOR, RECIPIENT, DEPOSITARY?, SERVICE\_MARKS, DOC+)>

<!ELEMENT RECIPIENT (CONTRAGENT)>

<!ELEMENT CONTRAGENT (CONTRAGENT\_CODE, CONTRAGENT\_NAME?, MAIL?)>

<!ELEMENT CONTRAGENT\_CODE (#PCDATA)>

<!ELEMENT SERVICE\_MARKS (SUBJECT?, COMMENT?, LETTER\_ID, CONTR\_LETTER\_ID, LETTER\_TYPE, CONVERSATION\_ID?, CREATE\_TIME, NDC\_RECEPT\_TIME?, NDC\_LETTER\_ID?, ORIG\_CONF\_SEND\_TIME?, NDC\_CHECKING?, RECIPIENT\_CHECKING?, RECIPIENT\_DELIV\_TIME?, RECIPIENT\_LETTER\_ID?, NDC\_RECIPIENT\_CONF\_DELIV\_TIME?, ORIG\_FINAL\_DELIV\_CONF\_SEND\_TIME?)>

<!ELEMENT SUBJECT (#PCDATA)>

<!ELEMENT DOC (FILE\_NAME, MAX\_DELIVERY\_TIME?, DOC\_TYPE, ORIGINAL\_FILE\_NAME?, IDENT\_CODE?, NDC\_STORAGE\_DOC\_ID?, NDC\_CHECKING?, RECIPIENT\_CHECKING?, RECIPIENT\_DOC\_ID?)>

<!ELEMENT DOC\_TYPE (#PCDATA)>

<!ELEMENT ORIGINAL\_FILE\_NAME (#PCDATA)>

* + 1. description of the elements and attributes used:

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Element name** | **Element attribute name** | **Narrative** |
|  | COVERING\_LETTER |  | A root element that contains all necessary information on the document package.  The element contains nested elements ORIGINATOR, RECIPIENT, DEPOSITARY, SERVICE\_MARKS and a recurring element DOC |
|  | RECIPIENT |  | The recipient of the Transit Electronic Document Package. The element contains a nested element CONTRAGENT |
|  | CONTRAGENT |  | A structure that contains information on the sender and the recipient of the Transit Electronic Document Package. The element contains a nested element CONTRAGENT\_CODE |
|  | CONTRAGENT\_CODE |  | The Recipient's depository code |
|  | SERVICE\_MARKS |  | An empty element that contains nested elements.  Mandatory elements: SUBJECT. |
|  | SUBJECT |  | The subject of the message; it contains the name of the financial message type in accordance with the Bank of Russia Unified Formats of Electronic Banking Messages: "SPFS.ED.\_type\_". |
|  | DOC |  | A structure that contains information on a single electronic document. It repeats once for each document in the package.  It contains the following mandatory elements: DOC\_TYPE, ORIGINAL\_FILE\_NAME |
|  | DOC\_TYPE |  | A transit package indicator: TRZT |
|  | DOC | ENCRYPTED | An indicator that the document in the package is encrypted.  YES if the package is encrypted, or NO otherwise |
| 10. | ORIGINAL\_FILE\_NAME |  | The original file name containing the document |

* 1. A single Transit Electronic Document Package shall be used to send a single Electronic Message that contains financial information to be transmitted to an SPFS User.
  2. The Customer shall encrypt the Electronic Communication using the Receiver Certificate.

1. **Processing of Transit Electronic Document Packages Received by the Service Bureau from the Client** 
   1. Provided that the initial and additional checks referred to in Appendix 4 to the EDI Rules have been successfully completed, the Service Bureau shall transmit the relevant Electronic Messages to the SPFS in accordance with the requirements and rules set out in the Bank of Russia's regulations and the electronic data interchange agreement between the Service Bureau and the Bank of Russia.

## Appendix 6

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

SAMPLE FORM

**Report  
on the Audit of Compliance with the Information Security Requirements in the SPFS Section**

**for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(year)*.**

*No \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ dated \_\_\_ \_\_\_\_\_\_\_\_ 20\_\_\_*

| **No.** | **Control description** | ***Findings***  *(comments)* |
| --- | --- | --- |
| **1.** | **Information protection in the course of access management** | |
|  | arrangement and control of the use of logical access subjects' user accounts | *The requirement is complied with / Description of any shortcomings identified* |
|  | arrangement and control of granting (revocation) and blocking of logical access | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to the use of user accounts and logical access rights, and logical access control | *The requirement is complied with / Description of any shortcomings identified* |
|  | identification and authentication of logical access subjects | *The requirement is complied with / Description of any shortcomings identified* |
|  | control and protection of identification and authentication data | *The requirement is complied with / Description of any shortcomings identified* |
|  | authorization (access control) for logical access purposes | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to identification, authentication or authorization for logical access | *The requirement is complied with / Description of any shortcomings identified* |
|  | arrangement and control of physical access to rooms in which information infrastructure components are installed | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to physical access | *The requirement is complied with / Description of any shortcomings identified* |
|  | documentation and control of information infrastructure resources and components; | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to changes in information infrastructure resources and components | *The requirement is complied with / Description of any shortcomings identified* |
| **2.** | **Protection of computer networks** | |
|  | segmentation and firewalling of local area networks | *The requirement is complied with / Description of any shortcomings identified* |
|  | protection of local area networks in the course of interaction with the Internet | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to changes in LAN security parameters | *The requirement is complied with / Description of any shortcomings identified* |
|  | monitoring and control of network traffic content | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to monitoring and control of network traffic content | *The requirement is complied with / Description of any shortcomings identified* |
|  | information protection against disclosure and modification when using wireless networks | *The requirement is complied with / Description of any shortcomings identified* |
|  | protection of local area networks when using wireless networks | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to the use of wireless networks | *The requirement is complied with / Description of any shortcomings identified* |
| **3** | **Monitoring the integrity and security of the information infrastructure** | |
|  | control to make sure information infrastructure components are not affected by known (described) information security vulnerabilities | *The requirement is complied with / Description of any shortcomings identified* |
|  | arrangement and control of the processes of hosting, storage and update of information infrastructure software | *The requirement is complied with / Description of any shortcomings identified* |
|  | composition and integrity control of information infrastructure software | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events related to the results of information infrastructure integrity and security controls | *The requirement is complied with / Description of any shortcomings identified* |
| **4** | **Protection against a malicious code** | |
|  | defence-in-depth to protect against a malicious code at different levels of information infrastructure | *The antivirus software (\_\_\_\_\_\_\_) is in operation; additionally, \_\_\_\_\_\_\_ is/are used / Description of any shortcomings identified* |
|  | arrangement and control of the application of tools designed for protection against a malicious code | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to protection against a malicious code | *The requirement is complied with / Description of any shortcomings identified* |
| **5** | **Prevention of data leakage** | |
|  | blocking of forbidden (and control of permitted) potential channels of data leakage | *The requirement is complied with / Description of any shortcomings identified* |
|  | control (analysis) of information transmitted via permitted potential channels of data leakage | *The requirement is complied with / Description of any shortcomings identified* |
|  | protection of machine-readable media | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to data leakage prevention | *The requirement is complied with / Description of any shortcomings identified* |
| **6** | **Information security incident management** | |
|  | monitoring of data concerning logged information security events, which is generated by information protection tools and systems and by information infrastructure components | *The requirement is complied with / Description of any shortcomings identified* |
|  | collection, protection and storage of data concerning logged information security events | *The requirement is complied with / Description of any shortcomings identified* |
|  | analysis of data concerning logged information security events | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to the processing of data concerning logged information security events | *The requirement is complied with / Description of any shortcomings identified* |
|  | detection and logging of information security incidents | *The requirement is complied with / Description of any shortcomings identified* |
|  | responding to information security incidents; | *The requirement is complied with / Description of any shortcomings identified* |
|  | storage and protection of information on information security incidents | *The requirement is complied with / Description of any shortcomings identified* |
|  | logging of information security events relating to detection of and responses to information security | *The requirement is complied with / Description of any shortcomings identified* |
| **7** | **Virtualization environment protection** | |
|  | identification, authentication and authorization (access control) for logical access purposes | *The requirement is complied with / Description of any shortcomings identified* |
|  | segmentation and firewalling of computer networks | *The requirement is complied with / Description of any shortcomings identified* |
|  | organisation of identification, authentication, authorisation (access delimitation) when logical access to virtual machines and server components of virtualisation is performed | *The requirement is complied with / Description of any shortcomings identified* |
|  | organising and controlling the communication and isolation of virtual machines | *The requirement is complied with / Description of any shortcomings identified* |
|  | organisation of virtual machine image protection | *The requirement is complied with / Description of any shortcomings identified* |
|  | registration of information security events related to access to virtual machines and server components of virtualisation | *The requirement is complied with / Description of any shortcomings identified* |
| **9** | **Information protection in case of remote logical access using mobile (portable) devices** | |
|  | Protection of information from disclosure and modification by remote access | *The requirement is complied with / Remote access is not used / Description of any shortcomings identified* |
|  | protection of internal computer networks in the case of remote access | *The requirement is complied with / Remote access is not used / Description of any shortcomings identified* |
|  | protection of information from disclosure and modification during its processing and storage on mobile (portable) devices | *The requirement is complied with / Remote access is not used / Description of any shortcomings identified* |
| **10** | **Documents defining the procedure for ensuring the protection of information during the transmission of electronic messages** | |
|  | processes of preparation, processing, transmission, and storage of electronic messages and protected information using information infrastructure | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | a list and rules of usage of information protection tools applied to control the integrity of and authenticate electronic messages at the stages of their generation (preparation), processing, transmission, and storage, including methods of using data encryption tools and managing data encryption tools' key information | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | a plan of actions to ensure continuity and/or disaster recovery of processes relating to electronic message interchange; | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | persons authorized to use data encryption tools | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | persons responsible for ensuring the functioning and security of data encryption tools (responsible data encryption tool users) | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | persons authorized to control cryptographic keys, including those responsible for generation of cryptographic keys and and the security of cryptographic keys | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | persons authorised to report detected incidents involving breaches of information security requirements in financial messaging | *The requirement is complied with, the description is available in \_\_\_\_\_\_\_\_\_ (document title) / The document needs to be updated; description of any shortcomings identified* |
|  | The details of persons authorized to report information security incidents detected during financial messaging shall be provided by the to the SPFS Service Bureau no later than the next day following their appointment or replacement | *The requirement is complied with / No changes took place during the reporting period / Description of any shortcomings identified* |
|  | Sending and receiving electronic messages of the Service Bureau's Client shall be maintained using a workstation designed for electronic message interchange | *The requirement is complied with / Description of any shortcomings identified* |
|  | Incoming and outgoing electronic messages shall be stored for at least five (5) years | *The requirement is complied with / Description of any shortcomings identified* |
| **11** | **Protection of electronic messages during their transmission to the Service Bureau by way of generating electronic messages and controlling their attributes in the information infrastructure** | |
|  | The segment in which electronic messages are generated and the segment in which their attributes are controlled in the Service Bureau's Client's information infrastructure shall be segregated, with different workstations and different employees being used in each of the segments | *The requirement is complied with / Description of any shortcomings identified* |
|  | The Client’s information infrastructure components used in the segment in which electronic messages are generated and those used in the segment in which electronic message attributes are controlled shall be installed in different computer network segments, including virtual segments. The process of permitted interaction between the said computer network segments has been duly documented and approved by the Client's information security function. | *The requirement is complied with / Description of any shortcomings identified* |
| **12** | **In the segment in which electronic messages are generated, the following steps shall be taken either on the basis of an underlying document in hard copy or electronic format, or on the basis of an incoming electronic message:** | |
|  | generation of an outgoing electronic message to be sent to the Service Bureau | *The requirement is complied with / Description of any shortcomings identified* |
|  | controlling the attributes of the outgoing electronic message to be sent to the Service Bureau; | *The requirement is complied with / Description of any shortcomings identified* |
|  | signing the outgoing electronic message to be sent to the Service Bureau, using for that purpose an electronic signature intended to be used in the segment in which electronic messages are generated, provided that the control of the electronic message attributes has returned positive results | *The requirement is complied with / Description of any shortcomings identified* |
|  | sending the outgoing electronic message to be sent to the Service Bureau to the segment in which electronic message attributes are controlled | *The requirement is complied with / Description of any shortcomings identified* |
| **13** | **In the segment in which electronic message attributes are controlled, the following steps shall be taken:** | |
|  | controlling the attributes of the outgoing electronic message to be sent to the Service Bureau to make sure those match the details of the underlying document in hard copy or electronic format or the incoming electronic message | *The requirement is complied with / Description of any shortcomings identified* |
|  | controlling duplicate outgoing electronic messages | *The requirement is complied with / Description of any shortcomings identified* |
|  | provided that the control of the electronic message attributes has returned positive results, sending the outgoing electronic message to the workstation designed for electronic message interchange, with further encryption of the electronic message at the application layer using the seven-layer basic model of open systems interconnection, as described in ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. Open Systems Interconnection. Basic Reference Model. The Basic Model | ***The requirement is complied with / Description of any shortcomings identified*** |
| **14** | **Protection of electronic messages during electronic messaging with the Service Bureau** | |
|  | Data protection tools shall be used which ensure mutual authentication and data encryption at the session layer (layer 5) and below layers, in accordance with the basic model of open systems interconnection, as described in ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. | *The requirement is complied with / Description of any shortcomings identified* |
|  | Interaction with the Service Bureau shall be maintained using hardware that have pre-approved unique remotely identifiable identification characteristics (IP address, DNS, etc.), and connecting any hardware with different identification characteristics shall be prohibited. | *The requirement is complied with / Description of any shortcomings identified* |
|  | For the purposes of analysis of measures applied to protect information in the course of data interchange, the Service Bureau's Client (a Client's authorized person) shall notify the Service Bureau of any information security incidents detected during the financial message interchange within eight business hours of the incident detection, by sending an information message by any method available. | *The requirement is complied with / No incident took place during the reporting period / Description of any shortcomings identified* |

The shortcomings identified need to be addressed by taking the following remedial actions:

| **No.** | **Remedial action description** | **Deadline, responsible person** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

The audit of compliance with the information security requirements in the SPFS Section has been conducted by:

*Representative of the information security function,   
Job title, name, surname \_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_

*Representative of IT support function,   
Job title, name, surname \_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_

*Representative of physical security function,   
Job title, name, surname \_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_

## Appendix 7

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

**List of the Client's Authorized Representatives**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Name, surname | Job title | Business telephone number | Email | Area of responsibility |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Job title)*  *L.S.* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Signed)* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(Name, surname)* |

## Appendix 8

to the Rules for the Provision of Services of the Bank of Russia Financial Messaging System Service Bureau

**Special aspects of technical support services for the Client**

1. The Service Bureau shall ensure the completion of Requests in due time subject to the timely provision of all necessary technical information to analyse the Request, including but not limited to the Software operation logs and error screenshots.
2. Means to submit Requests: email/telephone.
3. Methods and modes for logging Requests:

| Method for logging a Request | Incident | Service Request |
| --- | --- | --- |
| E-mail: transit-help@nsd.ru  Telephone: +7 (495) 956-09-34 | 24х7 | 24х7 |

1. Mode a Request is executed:

| Class of Request | Mode[[9]](#footnote-10) |
| --- | --- |
| High or Medium priority incident | 8.00-20.00 MSK on business days |
| Service Request | 9.00-18.00 MSK on business days |

1. Starting work on a Request: within 30 minutes
2. Software in service:

|  |  |
| --- | --- |
| **No.** | **Software** |
|  | Transit Terminal |

1. Timeframe for completion of Requests (from the moment all necessary information for completion of the Request is provided):

|  |  |  |  |
| --- | --- | --- | --- |
| Class of Request | Request type | **Requests related to the provision of electronic messaging between the Client and the Users of the SPFS** | **Requests not related to the provision of electronic messaging between the Client and the Users of the SPFS** |
| High priority Incident | Complete Software failure | 6 hours[[10]](#footnote-11) | - |
| Medium priority Incident | Failure to execute individual operations caused by errors in the Software | If the Incident can be rectified without changing the Software code - by the end of the operational day;  If the error in the Software code is detected - no later than the end of the operational day following the day of the request | Release N+1 day  (in accordance with NSD's release cycle, available on the website at: www.nsd.ru) |
| Service Request | | Two business days | 5 business days |

|  |  |
| --- | --- |
| **Impact of the Incident** | **Description** |
| High | Total unavailability of the Service. A service is considered totally unavailable when it is not available to all Clients. |
| Medium | Incident affecting the execution of the Client’s critical processes related to the provision of the Service, as well as partial inaccessibility of the Service. |

1. It is recommended to use the National Standard of the Russian Federation GOST R 57580.1-2017 *"Security of Financial (Banking) Operations.*  *Information Protection of Financial Organizations. Basic Set of Organizational and Technical Measures"*, as approved by Order No. 822-st of the Federal Agency for Technical Regulation and Metrology dated 8 August 2017 "*On the Approval of a National Standard of the Russian Federation" (M., FGUP "Standartinform", 2017).* [↑](#footnote-ref-2)
2. *The protection measure is included in the certificate if virtualisation technology is used in the electronic document transmission segment.* [↑](#footnote-ref-3)
3. *The protection measure is included in the certificate if the technology for remote logical access with the use of mobile (portable) devices is used in the electronic document transmission segment.* [↑](#footnote-ref-4)
4. *The protection measure is included in the certificate if electronic document transmission segment uses wireless network technology.* [↑](#footnote-ref-5)
5. *Similar to the reference in footnote 4* [↑](#footnote-ref-6)
6. *Similar to the reference in footnote 4* [↑](#footnote-ref-7)
7. *The protection measure is included in the certificate if virtualisation technology is used in the electronic document transmission segment.* [↑](#footnote-ref-8)
8. *The protection measure is included in the certificate if remote access technology is used in the electronic document transmission segment.* [↑](#footnote-ref-9)
9. If the time limit for a Request falls outside of Mode, the remaining time limit will be postponed to the next working day. [↑](#footnote-ref-10)
10. Subject to the Mode in which the Request is executed. [↑](#footnote-ref-11)