RULES OF ELECTRONIC DOCUMENT MANAGEMENT OF CFT ID CORPORATE INFORMATION SYSTEM

Rules come into effect since 6 december 2021

1. Terms and definitions

1.1 **CFT ID SYSTEM ("SYSTEM")** - corporate information system established by Closed Joint Stock Company "Tsenter Tsifrovykh Sertificatov" (Закрытое акционерное общество «Центр Цифровых Сертификатов»), TIN 5407187087 (hereinafter referred to as the «**SYSTEM OPERATOR**», the «**OPERATOR**») to provide contractual and technologic conditions necessary to create and develop financial and information electronic services provided by the **SYSTEM OPERATOR** and **ORGANIZERS OF ASSOCIATED SERVICES TO THE SYSTEM USERS**.

1.2 **SYSTEM PARTICIPANT ("PARTICIPANT")** – is the **OPERATOR OF THE SYSTEM**, **ORGANIZER OF ASSOCIATED SERVICE, CLIENT OF THE SYSTEM** or **SYSTEM USER** in accordance with these **RULES OF ELECTRONIC DOCUMENT MANAGEMENT OF CFT ID CORPORATE INFORMATION SYSTEM (RULES).**

1.3 **ORGANIZER OF ASSOCIATED SERVICE** – is the legal entity that has signed an accession agreement with the **SYSTEM OPERATOR** as the **ORGANIZER OF ASSOCIATED SERVICE** and provides financial and/or information electronic services to **SYSTEM USERS** through the **SYSTEM**.

1.4 **ASSOCIATED SERVICE** – is a part of the **SYSTEM** used by **ORGANIZER OF ASSOCIATED SERVICE** to provide financial and/or information services to **SYSTEM USERS. ASSOCIATED SERVICE** uses the **SYSTEM** to perform identity check or **ELECTRONIC DOCUMENT MANAGEMENT** in accordance herewith.

1.5 **SYSTEM CLIENT (CLIENT)** – is a legal entity acceded to the **SYSTEM** as a **SYSTEM CLIENT** in accordance with the procedure established hereby.

1.6 **EMPLOYEE OF THE SYSTEM CLIENT** – is an individual employed or otherwise authorized by the **SYSTEM CLIENT** and empowered to perform transactions via the **SYSTEM** on behalf of the **SYSTEM CLIENT**.

1.7 **ADMINISTRATOR** – is a **SYSTEM USER** responsible for registration, editing and managing **USER ACCOUNTS OF EMPLOYEES OF THE SYSTEM CLIENT** in the **SYSTEM**.

1.8 **USER ACCOUNT** – is a set of **IDENTIFICATION AND AUTHENTICATION DATA** that uniquely determine a **USER** in the **SYSTEM**.

1.9 **IDENTIFICATION DATA** – means the data allowing to determine personality of the **SYSTEM USER** within the framework of the **SYSTEM**.

1.10 **AUTHENTICATION DATA** – means the data provided or otherwise used by the **SYSTEM USER** in the process of **AUTHENTICATION** and due to their non-public nature allowing to unambiguously determine if provided **IDENTIFICATION DATA** actually correspond to the **SYSTEM USER**.

1.11 **PERSONAL AREA** – means part of the **SYSTEM** used by the **USER** to amend **IDENTIFICATION** and **AUTHENTICATION DATA**. **PERSONAL AREA** can be found on the website https://cftid.perevod-korona.com.

1.12 **AUTHENTICATION** – means the procedure applied to check if the **IDENTIFICATION DATA** provided by the **USER** actually correspond to the **USER** by comparing **AUTHENTICATION DATA** provided by the **SYSTEM USER** with **AUTHENTICATION DATA** (either with their converted values or data unambiguously related to the **AUTHENTICATION DATA**) stored in the **SYSTEM**.

1.13 **IDENTIFICATION** – means the procedure for establishing unambiguous affiliation and use of **LOGIN** by the corresponding **SYSTEM USER**.

1.14 **COMPROMISE OF AUTHENTICATION DATA, TOKEN** – means situation upon which confidentiality of **AUTHENTICATION DATA** and/or **TOKEN** is broken, or the owner reports on the case of unauthorized use or possible of **AUTHENTICATION DATA** or **TOKEN** by unauthorized persons.

1.15 **SYSTEM USER (USER)** – **EMPLOYEE OF THE SYSTEM CLIENT** registered with the **SYSTEM**.

1.16 **TOKEN** – means a set of data automatically generated by the **SYSTEM** in case of successful **IDENTIFICATION** and **AUTHENTICATION** uniquely related to the **SYSTEM USER** and allowing to confirm the fact of generation of an **ELECTRONIC DOCUMENT** by a definite **SYSTEM USER**.

1.17 **SIMPLE ELECTRONIC SIGNATURE** – means a detail of an **ELECTRONIC DOCUMENT** required to secure **ELECTRONIC DOCUMENT** from forgery and confirm that a **SIMPLE ELECTRONIC SIGNATURE** was generated by **SYSTEM USER**.

1.18 **ENHANCED ELECTRONIC SIGNATURE –** means a detail of an **ELECTRONIC DOCUMENT** required to secure **ELECTRONIC DOCUMENT** from forgery, to ensure integrity of an **ELECTRONIC DOCUMENT** and to confirm that an **ENHANCED ELECTRONIC SIGNATURE** was generated by **SYSTEM USER.**

1.19 **ELECTRONIC SIGNATURE** – means under the **RULES** a **SIMPLE ELECTRONIC SIGNATURE** and an **ENHANCED ELECTRONIC SIGNATURE**, unless otherwise expressly stated otherwise.

1.20 **LOGIN** – means a unique **SYSTEM** identifier attached to a **SYSTEM USER** and uniquely related to **IDENTIFICATION DATA** of this **SYSTEM USER**.

1.21 **ELECTRONIC MESSAGE** – means an entire set of structured data useful for **SYSTEM PARTICIPANTS**. Information in **ELECTRONIC MESSAGE** is represented in electronic digital format allowing computer processing, transferring via communication channels and storing on machine-readable carriers.

1.22 **ELECTRONIC DOCUMENT –** means an **ELECTRONIC MESSAGE**, signed with a **SIMPLE ELECTRONIC SIGNATURE** or an **ENHANCED ELECTRONIC SIGNATURE** in accordance with the order of **ELECTRONIC DOCUMENT MANAGEMENT**, provided herein. The format of **ELECTRONIC DOCUMENT** used under **ELECTRONIC DOCUMENT MANAGEMENT** shall be determined in accordance with the technical process of the **SYSTEM** or the **ASSOCIATED SERVICE**.

1.23 **SYSTEM LOG** – means database necessary for continuous recording of actions taken under **USER ACCOUNTS** of **SYSTEM USERS,** facts of **IDENTIFICATION AND AUTHENTICATION** and facts of issuance, checking and **COMPROMISING** of **TOKENS** with the indication of all data contained in **TOKENS, USER IDENTIFICATION DATA,** date and time of the actions taken. **SYSTEM LOG** is maintained by **SYSTEM OPERATOR** in electronic format in the standard operating mode continuously and automatically. **SYSTEM LOG** format excludes modifying and deleting entries on recorded events as well as making records in a manner

not provided for by the technical process of the **SYSTEM**. The purpose of maintaining a **SYSTEM LOG** is establishment of an unambiguous connection between **SYSTEM USERS** and **TOKENS** issued to them, organization of **SIMPLE ELECTRONIC SIGNATURE** or **ENHANCED ELECTRONIC SIGNATURE** verification procedure, detection of situations connected with unauthorized actions, monitoring of the events in order to control, resolution of disputable and conflict situations related to operation of the **SYSTEM**. **SYSTEM PARTICIPANTS** recognize the data contained in the **SYSTEM LOG** true and serving as a basis for dispute resolution. Records in a **SYSTEM LOG** are stored not less than 5 (five) years since they are recorded in a **SYSTEM LOG**.

1.24 **SENDER OF ELECTRONIC DOCUMENT** – means a **SYSTEM PARTICIPANT** that sends an **ELECTRONIC DOCUMENT** via the **SYSTEM**.

1.25 **ELECTRONIC DOCUMENT MANAGEMENT, E-DOCUMENT MANAGEMENT** – means an **ELECTRONIC DOCUMENT** exchange performed in the **SYSTEM** in accordance with these **RULES** and the rules of **ASSOCIATED SERVICES**.

1.26 **TOKEN CONTROL INTERFACE** – means a part of the **SYSTEM** generated to verify **TOKEN**.

1.27 **AUTHENTICATION INTERFACE** – means a part of the **SYSTEM** used to perform **IDENTIFICATION** and **AUTHENTICATION** procedures.

1.28 **USER CONTROL INTERFACE** – means a part of the **SYSTEM** designed for registration, editing and management of **USER ACCOUNTS** by **CLIENT ADMINISTRATOR** by directing requests to the **OPERATOR** (the list of requests is presented in **APPENDIX 2** to these **RULES**).

1.29 **RECEIVER OF ELECTRONIC DOCUMENT** – means a **PARTICIPANT** receiving an **ELECTRONIC DOCUMENT** via the **SYSTEM**.

1.30 **BUSINESS TELEPHONE NUMBER** – is a number used by an **EMPLOYEE OF THE SYSTEM CLIENT** in order perform assigned duties.

1.31 **MOBILE PHONE NUMBER** – customer number of mobile radio belonging to an **EMPLOYEE OF THE SYSTEM CLIENT** under an agreement with a cellular mobile operator.

1.32 **TOKEN AUTHORISATION CODE –** means information in electronic format being part of **TOKEN** and generated upon issuance of **TOKEN** by **THE SYSTEM OPERATOR**, which is a random variate unique among all generated **TOKEN AUTHORISATION CODES** and is aimed to prevent brute force attack. Results of matching of **TOKEN AUTHORISATION CODE** with the **SYSTEM** data shall be provided in the **TOKEN CONTROL INTERFACE** in applying for **TOKEN** verification.

1.33 **SINGLE-USE PASSWORD** – a unique set of symbols used to authenticate a **USER** by and confirm generation of a **USER ACCOUNT**.

1.34 **PASSWORD** – means a confidential character sequence known by a **USER** only and used for **AUTHENTICATION** through **PASSWORD.**

2. Scope of the Rules

2.1 These **RULES** and **APPENDIXES** hereto set general principles of **ELECTRONIC DOCUMENT** exchange between the **SYSTEM PARTICIPANTS**. Requirements for execution and content of **ELECTRONIC DOCUMENTS,** their format and details, processing sequence, implementation and storage peculiarities are determined hereby and supplementary agreements signed between respective **PARTICIPANTS** as well as by the rules of **ORGANIZERS OF ASSOCIATED SERVICES**. Requirements of supplementary agreements concluded between the **SYSTEM OPERATOR** and the respective **PARTICIPANTS**, as well as the rules of

ORGANIZERS OF ASSOCIATED SERVICES must not contravene the principles established in these **RULES**.

2.2 These **RULES** shall apply unless otherwise provided for by legislation or other regulatory legal acts of the Russian Federation including laws and regulations of the Bank of Russia.

2.3 **SYSTEM PARTICIPANT** may only be a limited group of persons who have acceded to the **SYSTEM** and the **RULES OF ELECTRONIC DOCUMENT MANAGEMENT OF THE "CFT ID" SYSTEM** (hereinafter referred to as "**RULES**") in accordance with the procedure established by the **RULES** (Section 3). A **PARTICIPANT** can accede to the **RULES** only if he agrees with the **RULES** and conditions of accedence to the **SYSTEM** and meets the criteria contained herein. An applicant may receive a notification with a waiver to accede with no reason given.

2.4 These **RULES** do not handle the issues of **ELECTRONIC MESSAGE EXCHANGE** being not **ELECTRONIC DOCUMENTS** in accordance herewith.

3. Procedure for joining the System of the System participants (conclusion of an agreement), entry into force of these Rules and amending hereof.

3.1. These **RULES** including all **APPENDIXES** hereto are approved by the **SYSTEM OPERATOR**. **SYSTEM OPERATOR** shall on unilateral basis introduce modifications.

3.2. These **RULES** shall come into effect in respect of the **EMPLOYEE OF THE SYSTEM CLIENT** from the moment of its registration in the **SYSTEM** in case of successful verification of data of **EMPLOYEE OF THE SYSTEM CLIENT**. The rules shall apply to the **SYSTEM CLIENT, SYSTEM USER, ORGANIZER OF THE ASSOCIATED SERVICE,** and other **SYSTEM PARTICIPANTS** only in case of their participation in operation of the respective **ASSOCIATED SERVICE**.

3.3. These **RULES** shall come into effect in respect of **ORGANIZER OF ASSOCIATED SERVICE** after execution of an agreement on accession to the **SYSTEM** as an **ORGANIZER OF ASSOCIATED SERVICE** with the **SYSTEM OPERATOR** or an authorized person of the **SYSTEM OPERATOR.** The **RULES** apply in respect of the **ORGANIZER OF ASSOCIATED SERVICE** throughout the period of validity of the agreement on accession to the **SYSTEM** as an **ORGANIZER OF ASSOCIATED SERVICE**.

3.4. By acceding hereto **SYSTEM PARTICIPANT** shall sign the accession agreement in the form of **APPENDIX 1** to these **RULES**, accept their terms and conditions in full in the order, provided for by article 428 of the Civil Code of the Russian Federation and undertake to comply with them, and also recognize that receipt of the **ELECTRONIC DOCUMENT** signed in accordance herewith with **SIMPLE ELECTRONIC SIGNATURE** or **ENHANCED ELECTRONIC SIGNATURE** of the **SYSTEM PARTICIPANT** shall be legally equivalent to receipt of its hard copy authenticated by personal handwritten signature of the **SYSTEM PARTICIPANT/**authorized persons of the **SYSTEM PARTICIPANT** and bearing a seal of the **SYSTEM PARTICIPANT.** The obligations provided for hereby shall be effective in case **SIMPLE ELECTRONIC SIGNATURE** or **ENHANCED ELECTRONIC SIGNATURE** is generated using the **SYSTEM**'s technical process.

4. Procedure for registration of the Employee of the System Client with the System

4.1 Registration of the Employee/ Employees of the System Client

4.1.1 Depending on the status in which the **EMPLOYEE/ EMPLOYEES OF** the **SYSTEM CLIENT** is required to be registered the **SYSTEM CLIENT** shall send to the **OPERATOR** a hard copy application in the form provided for in the Internet on the website http://cft.group/company-group/contracts, which is to be signed by an authorized person of the **SYSTEM CLIENT** and sealed (unless otherwise provided for by law) of the **SYSTEM CLIENT:**

- for registration of an Employee of the **SYSTEM CLIENT** as an **ADMINISTRATOR –** in order to register an **EMPLOYEE** of the **SYSTEM CLIENT** in the **SYSTEM** as an **ADMINISTRATOR** (application in the form of **APPENDIX 3** to these **RULES**);
- for registration of an **EMPLOYEE/ EMPLOYEES** of the **SYSTEM CLIENT** as a **SYSTEM USER/USERS –** in order to register an **EMPLOYEE/EMPLOYEES** of the **SYSTEM CLIENT** as a **SYSTEM USER/USERS** (application in the form of **APPENDIX 4** to these **RULES**).

4.1.2 If a **SYSTEM CLIENT** and an **ORGANIZER OF ASSOCIATED SERVICE** need to apply any special measures of data protection (**ENHANCED ELECTRONIC SIGNATURE** or any additional data security tools), a **SYSTEM CLIENT** shall prior to registration of an **EMPLOYEE/CLIENT'S EMPLOYEES** send a paper Questionnaire on special security measures applied by a **SYSTEM CLIENT** and an **OPERATOR** to the **OPERATOR** in the form (APPENDIX 8 hereto) available on the website http://service.cft.ru/Pages/agreements.aspx or in another form as agreed upon with an **OPERATOR.**

4.1.3 Depending of the **USER ACCOUNT** confirmation method the message confirming creation of a **USER ACCOUNT** shall be sent to an e-mail address or to **MOBILE PHONE NUMBER**. **USER ACCOUNT/ACCOUNTS** confirmation shall be performed in accordance with section 4.3 hereof.

4.2 Registration of an Employee of the System Client by an Administrator

4.2.1 **SYSTEM CLIENT** represented by the **ADMINISTRATOR** has the right to conduct the registration of an **EMPLOYEE/EMPLOYEES OF THE SYSTEM CLIENT** with the **SYSTEM:**

- via **USER CONTROL INTERFACE** (except for registration of an **EMPLOYEE OF THE SYSTEM CLIENT** as an **ADMINISTRATOR**). Registration shall be performed in two stages: **ADMINISTRATOR** creates a **USER ACCOUNT** and **EMPLOYEE OF THE SYSTEM CLIENT** confirms creation of a **USER ACCOUNT**. Registration shall be considered completed only if both stages are successfully finished.

4.2.2 **ADMINISTRATOR** is not authorized to register **EMPLOYEES OF THE SYSTEM CLIENT** with the **SYSTEM** as **ADMINISTRATORS.** Registration as **ADMINISTRATOR** shall be made only in accordance with clause 4.1. of these **RULES**.

4.2.3 **ADMINISTRATOR** may register the **EMPLOYEES OF THE SYSTEM CLIENT** only of the **SYSTEM CLIENT** on whose behalf he acts.

4.3 Creation of USER ACCOUNT

4.3.1 **ADMINISTRATOR** via **USER CONTROL INTERFACE** shall send a request for registration of **EMPLOYEE OF THE SYSTEM CLIENT** with the **SYSTEM** or the **SYSTEM CLIENT**

shall send to the **OPERATOR** a request for registration of **EMPLOYEE/ EMPLOYEES OF THE SYSTEM CLIENT** in hard copy.

4.3.2 Upon registration of **EMPLOYEE/EMPLOYEES OF THE SYSTEM CLIENT** the following data shall be specified:

4.3.2.1 Surname, name, patronymic (unless otherwise is provided for by legislation or national custom);

4.3.2.2 Full company name of the **SYSTEM PARTICIPANT**;

4.3.2.3 **LOGIN**;

4.3.2.4 Method of **AUTHENTICATION** (list of possible methods is provided for herein);

4.3.2.5 Method applied to confirm creation of a **USER ACCOUNT** (by email or **MOBILE PHONE NUMBER**). If the method applied to confirm creation of the **USER ACCOUNT** is not stated the method applied by default shall be confirmation by **MOBILE PHONE NUMBER.** In case the **MOBILE PHONE NUMBER** has not been provided the confirmation method applied shall be confirmation by email.

4.3.2.6 **MOBILE PHONE NUMBER**;

4.3.2.7 Email address;

4.3.3 Prior to registration of an **EMPLOYEE/CLIENT'S EMPLOYEES** if a **SYSTEM CLIENT** needs to apply any special measures of data protection (including cases, when an **ENHANCED ELECTRONIC SIGNATURE** has be applied by a **SYSTEM CLIENT**), a **SYSTEM CLIENT** shall provide an **OPERATOR** with data required to apply special protection measures and ensure implementation thereof upon agreement with an **OPERATOR.**

4.3.4 Details specified in clauses 4.3.2.1-4.3.2.2, 4.3.2.6 or 4.3.2.7 (depending on the method applied to confirm creation of a **USER ACCOUNT**) hereof are mandatory. Registration with the **SYSTEM** shall not be performed without such data.

4.3.5 In case of sending a request/application for registration of **EMPLOYEE/EMPLOYEES OF THE SYSTEM CLIENT**, the **OPERATOR** assigns a unique **LOGIN** to **EMPLOYEE OF THE SYSTEM CLIENT** on its own.

4.3.6 If email is specified as a method to confirm creation of a **USER ACCOUNT**, it is obligatory to specify the email address.

4.3.7 **ADMINISTRATOR/** the **SYSTEM CLIENT** cannot register an **EMPLOYEE OF THE SYSTEM CLIENT** with full company name of the **SYSTEM CLIENT** that is different from full company name of **SYSTEM CLIENT** on behalf of which **ADMINISTRATOR** performs transaction in the **SYSTEM**.

4.3.8 **SYSTEM CLIENT** shall be responsible for validity and accuracy of information provided to the **SYSTEM** by **USERS**, which perform transactions in the **SYSTEM** on behalf of this **CLIENT**.

4.4 Confirmation of User Account creation:

4.4.1 In case of successful creation of a **USER ACCOUNT** if confirmation by email is chosen as a method applied to confirm creation of a **USER ACCOUNT**, the procedure of **USER ACCOUNT** creation shall be performed in the following order:

4.4.1.1 A notification of necessity to confirm the **USER ACCOUNT** and **LOGIN** of the **EMPLOYEE** of the **SYSTEM CLIENT** shall be sent to the email address specified upon creation of **USER ACCOUNT**

4.4.1.2 Upon receipt of the notification according to clause 4.4.1.1 hereof the **EMPLOYEE** of the **SYSTEM CLIENT** is to follow a link https://cftid.perevod-korona.com/cftid_entry/emailpass.

Further, on the specified page, the **EMPLOYEE** of the **SYSTEM CLIENT** enters **LOGIN** and email address indicated upon registration, requests **SINGLE-USE PASSWORD** and enters the received **SINGLE-USE PASSWORD.** After entering the **SINGLE-USE PASSWORD** an **EMPLOYEE OF THE SYSTEM CLIENT** enters **AUTHENTICATION DATA** in accordance with the selected upon registration method of **AUTHENTICATION**.

4.4.2 In case of successful creation of **USER ACCOUNT** and confirmation thereof by **MOBILE PHONE NUMBER**, the procedure of **USER ACCOUNT** creation shall be performed in the following order:

4.4.2.1 An SMS-message with a **LOGIN** of the **EMPLOYEE** of the **SYSTEM CLIENT** shall be sent to the **MOBILE PHONE NUMBER** specified upon registration;

4.4.2.2 Upon receipt of the SMS-message according to clause 4.4.2.1 of these **RULES,** the **EMPLOYEE** of the **SYSTEM CLIENT** is to follow a link https://cftid.perevod-korona.com/cftid_entry/otppass. Further, on the specified page, the **EMPLOYEE** of the **SYSTEM CLIENT** enters **LOGIN** and **MOBILE PHONE NUMBER** indicated upon registration, requests **SINGLE-USE PASSWORD** and enters the received **SINGLE-USE PASSWORD.** After entering the **SINGLE-USE PASSWORD** an **EMPLOYEE OF THE SYSTEM CLIENT** enters **AUTHENTICATION DATA** in accordance with the selected upon registration method of **AUTHENTICATION** .

4.4.3 Confirming the creation of **USER ACCOUNT** is also possible in another way provided by the **SYSTEM**.

4.4.4 By entering of the **AUTHENTICATION DATA,** the **EMPLOYEE OF THE SYSTEM CLIENT** confirms that he (she) is familiarized with the rules of electronic document management of **CFT ID SYSTEM. SYSTEM CLIENT** is obliged to familiarize its **EMPLOYEES** with the rules of **CFT ID SYSTEM** and assumes all risks and negative consequences for the actions/omissions of its **EMPLOYEES** caused by ignorance of the rules of **CFT ID SYSTEM.**

4.4.5 In case a **PASSWORD/SINGLE-USE PASSWORD** has been selected as the method of **AUTHENTICATION, EMPLOYEE OF THE SYSTEM CLIENT** shall create and enter in the confirmation form the data provided for this **AUTHENTICATION** method;

4.4.6 As soon as **AUTHENTICATION DATA** are entered and successfully reviewed for their compliance with the requirements imposed to **AUTHENTICATION DATA,** the **USER ACCOUNT** shall be considered to be successfully generated and the **EMPLOYEE OF THE SYSTEM CLIENT** shall be considered to be registered with the **SYSTEM**.

4.5 Editing USER ACCOUNT details

4.5.1 Editing **USER ACCOUNT** details shall be performed by the **USER** in the **SYSTEM PERSONAL AREA** or by the **ADMINISTRATOR** with the use of **USER CONTROL INTERFACE** or by the **OPERATOR** at the request of the **CLIENT**.

The **USER** is obliged to immediately edit the **USER ACCOUNT** details provided earlier in the event of their change.

4.5.2 **USER** of the **SYSTEM** can amend the following data in the **PERSONAL AREA**:

4.5.2.1 Surname, name, patronymic (unless otherwise is provided for by legislation or national custom) of the **USER**;

4.5.2.2 Email address;

4.5.2.3 **MOBILE PHONE NUMBER**;

4.5.2.4 **AUTHENTICATION DATA** corresponding to the selected method of **AUTHENTICATION**;

4.5.3 **ADMINISTRATOR** can use **USER CONTROL INTERFACE** to edit the following data:

4.5.3.1 Surname, name, patronymic of the **USER** (unless otherwise provided for by legislation or national custom);

4.5.3.2 Full company name of the **SYSTEM CLIENT**;

4.5.3.3 List of **AUTHENTICATION** methods used to perform **AUTHENTICATION**;

4.5.3.4 Email address;

4.5.3.5 **MOBILE PHONE NUMBER**;

4.5.4 At the request of the **CLIENT,** an **OPERATOR** can edit the following data:

4.5.4.1 Surname, name, patronymic (unless otherwise is provided for by legislation or national custom) of the **USER**;

4.5.4.2 E-mail address;

4.5.4.3 **MOBILE PHONE NUMBER**;

4.5.4.4 **USER ACCOUNT** confirmation method.

4.5.5 In order for the **OPERATOR** to modify the **USER ACCOUNT** data, the **CLIENT** must send an Application for amending **USER ACCOUNT** (The **APPENDIX N 5** to these **RULES**). The Application for amending **USER ACCOUNT** should be sent to the **OPERATOR** in hard copy.

4.5.6 When editing the data of **USER ACCOUNT**, **ADMINISTRATOR** is obliged to countercheck and confirm their validity. **SYSTEM USER** must specify valid data upon editing the data of **USER ACCOUNT**. Submission of false data is prohibited. Wrong data specified by a **SYSTEM USER** can lead to unavailability to use the **SYSTEM**.

4.5.7 **ADMINISTRATOR** shall lock out the **USER ACCOUNT** of the **SYSTEM USER** in case this **USER ACCOUNT** belongs to the **EMPLOYEE** of the **SYSTEM CLIENT** whose employment has been terminated. In case the **SYSTEM CLIENT** acts within the **SYSTEM** without **ADMINISTRATOR** or **ADMINISTRATOR** cannot perform the lock out of the **USER ACCOUNT** of the **SYSTEM USER,** the lock out of the **USER ACCOUNT** of the **SYSTEM USER,** whose employment has been terminated, is to be performed by the **CLIENT. USER ACCOUNT** of the **ADMINISTRATOR** may be locked out only by the **CLIENT** or the **OPERATOR,** in the manner prescribed by clause 4.6. of these **RULES**.

ADMINISTRATOR via **USER CONTROL INTERFACE** submits to the **SYSTEM** the request for locking out of the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** or the **SYSTEM CLIENT** submits to the **OPERATOR** the request for locking out of the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** in hard copy **(APPENDIX 6** hereto**).** The request or the application for locking out of the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** is to be submitted to the **OPERATOR** not later than the date of the last working day of the **EMPLOYEE** of the **SYSTEM CLIENT.** The lock out of the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** is performed by the **OPERATOR** not later than the day following the working day when the request or the application for locking out of the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** has been receipt.

ADMINISTRATOR shall have the right to unlock the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** blocked as a result of sending an application to the **OPERATOR** to lock out the **USER ACCOUNT** of the **EMPLOYEE** of the **SYSTEM CLIENT** or locked out by the **OPERATOR** in the manner specified in clause 4.6. of these **RULES.**

4.5.8. **SYSTEM USER** has a right to amend the **PASSWORD** by making changes on the **SYSTEM** page available at: https://cftid.perevod-korona.com/cftid_entry/repass using the method of confirming the **USER ACCOUNT** by this **SYSTEM USER**.

4.6. Locking out of USER ACCOUNT by the OPERATOR

4.6.1. The **OPERATOR** has a right to lock out the **USER ACCOUNT** of the **SYSTEM USER**, with the possibility of it unlocking in the future, in case the **USER** of this **USER ACCOUNT** has not performed operations in the **SYSTEM** for 3 (three) months.

4.6.2. The **OPERATOR** has a right to lock out the **USER ACCOUNT** of the **SYSTEM USER**, without possibility of it unlocking in the future, in case the **USER** of this **USER ACCOUNT** has not performed operations in the **SYSTEM** for 3 (three) years.

4.6.3. **USER ACCOUNT** locked out in accordance with the terms of clause 4.6.1. of these **RULES** can be unlocked by the **ADMINISTRATOR** via **USER CONTROL INTERFACE** or by the **CLIENT** via submitting an application for unlocking **USER ACCOUNT (APPENDIX 7** hereto**)**. An application for unlocking **USER ACCOUNT** should be directed to the **OPERATOR** in hard copy.

USER ACCOUNT of the **ADMINISTRATOR** may be unlocked only by the **CLIENT** via submitting an application for unlocking **USER ACCOUNT (APPENDIX 7** hereto**)**.

5. Operation of the System

5.1 Identification

5.1.1. An **EMPLOYEE OF THE SYSTEM CLIENT** shall be assigned a **LOGIN** upon registration with the **SYSTEM**.

5.1.2. **LOGIN** shall be used for **IDENTIFICATION OF THE SYSTEM USER**.

5.2 Authentication

5.2.1 **AUTHENTICATION** of the **SYSTEM USER** is possible only after successful registration with the **SYSTEM**.

5.2.2 For **AUTHENTICATION** a **SYSTEM USER** shall enter **LOGIN** and **AUTHENTICATION DATA** in the **AUTHENTICATION INTERFACE**. The following data can be used as **AUTHENTICATION DATA**:

5.2.2.1 **PASSWORD**;

5.2.2.2 **SINGLE-USE PASSWORD**;

5.2.3 **AUTHENTICATION** may be performed by any **AUTHENTICATION** method determined in section 5.2.2 hereof or by a combination of the methods in accordance with the description provided in section 5.2.6 hereof. The set of used **AUTHENTICATION DATA** shall be determined by the **SYSTEM PARTICIPANT**.

5.2.4 **IDENTIFICATION** and **AUTHENTICATION** shall be considered to be performed successfully if the **IDENTIFICATION** and **AUTHENTICATION DATA** entered by the **SYSTEM USER** match **IDENTIFICATION** and **AUTHENTICATION DATA** of the **USER** stored and saved by the **SYSTEM**.

5.2.5 **SYSTEM OPERATOR** has a right to set mandatory requirements to the **SYSTEM PARTICIPANTS** regarding composition, frequency of editing and other parameters of **AUTHENTICATION DATA** in order to increase security level in the **SYSTEM**.

5.2.6 Depending on the method, **AUTHENTICATION** corresponds to a number of actions, described below:

5.2.6.1 Upon **AUTHENTICATION** using the **PASSWORD,** a **LOGIN** assigned to a **SYSTEM USER** and the **PASSWORD** stored in the **SYSTEM** shall be matched with the **LOGIN-PASSWORD** pair specified by the **USER** upon **AUTHENTICATION** in the **SYSTEM**;

5.2.6.2 Upon **AUTHENTICATION** using a **SINGLE-USE PASSWORD,** a **SINGLE-USE PASSWORD** sent at a given time via a pre-configured channel for obtaining a **SINGLE-USE PASSWORD** and entered by the **USER,** shall be matched with the **SINGLE-USE PASSWORD** provided to the **USER** in a given period of time. The **AUTHENTICATION** method provided in this clause may be applied only in combination with other methods of **AUTHENTICATION**. The **USER** can set up the channel for receiving the **SINGLE-USE PASSWORD** via **PERSONAL AREA** or at the first logon to the **SYSTEM**.

5.2.7 The **USER** shall maintain confidentiality of **AUTHENTICATION DATA**. The **CLIENT** shall ensure that the **USERS** comply with the **AUTHENTICATION DATA** confidentiality requirements**.**

5.2.8 **SINGLE-USE PASSWORD** has a limited validity in accordance with the **SYSTEM's** technical process.

5.2.9 **SYSTEM OPERATOR** shall define possibility of **AUTHENTICATION** using any of the provided methods.

5.2.10 **AUTHENTICATION DATA** in the **SYSTEM** are stored in a modified form excluding the possibility to use stored data for **AUTHENTICATION**. Stored **AUTHENTICATION DATA** are used for matching with the **AUTHENTICATION DATA** entered by the **USER**.

5.3 Issuance of a Token

5.3.1 In case of successful **IDENTIFICATION** and **AUTHENTICATION, TOKEN** shall be issued to a **SYSTEM USER. TOKEN** shall be automatically generated by the **SYSTEM OPERATOR**.

5.3.2 User-side **TOKEN** shall be stored in accordance with the technical process of the **SYSTEM**.

5.3.3 Validity of **TOKEN** is limited by **TOKEN** expiration time in accordance with the **SYSTEM** technical process.

5.3.4 **TOKEN** contains the following details:

5.3.4.1 Unique identifier of the **SYSTEM USER**;

5.3.4.2 Unique identifier of **TOKEN**;

5.3.4.3 Time of creation of **TOKEN**;

5.3.4.4 **TOKEN** expiration time;

5.3.4.5 **TOKEN AUTHORISATION CODE**;

5.3.5 The **USER** shall maintain confidentiality of **TOKEN** during the **TOKEN** validity period. The **CLIENT** shall eliminate the possibility of **TOKEN** confidentiality compromise at **USERS'** workplaces**.**

5.4 Work in the Personal area and USER CONTROL INTERFACE

5.4.1 Access to **SYSTEM PERSONAL AREA** and **USER CONTROL INTERFACE** shall be performed via **AUTHENTICATION INTERFACE** in accordance with sections 5.1-5.3 hereof.

5.4.2 Operation in the **PERSONAL AREA** is an **ELECTRONIC DOCUMENT EXCHANGE** between a **USER** and a **SYSTEM** in the format specified in **APPENDIX 2** and in accordance with these **RULES**.

5.4.3 Operation in the **USER CONTROL INTERFACE** is an **ELECTRONIC DOCUMENT EXCHANGE** between a **USER** and a **SYSTEM** in the format specified in **APPENDIX 2** and in accordance with these **RULES**.

5.5 Transfer of electronic documents

5.5.1 **SYSTEM PARTICIPANTS** shall transfer **ELECTRONIC DOCUMENTS,** including **TOKENS** being part of **ELECTRONIC DOCUMENTS,** only by an enforced path that ensures confidentiality upon data transfer. Arrangement of an enforced path shall be determined by the technical process of the **SYSTEM** or the **ASSOCIATED SERVICE** within which the transfer of **ELECTRONIC DOCUMENTS** is performed.

6. Electronic document

6.1 Requirements regarding to an Electronic Document

6.1.1. **ELECTRONIC DOCUMENT** created in the **SYSTEM** shall be legally binding and imply legal consequents specific for the given **ELECTRONIC DOCUMENT** in accordance herewith, with the rules of the **ASSOCIATED SERVICE** and effective legislation of the Russian Federation as well as contractual relations between **SYSTEM PARTICIPANTS**.

6.1.2. **ELECTRONIC DOCUMENT** used in the **SYSTEM** shall be considered duly executed in case it complies with the legislation of the Russian Federation, these **RULES,** the rules of the **ASSOCIATED SERVICES**, and supplementary agreements signed between **SYSTEM PARTICIPANTS**, if any.

6.1.3. **ELECTRONIC DOCUMENT** shall be generated in the format provided therefor in accordance with the technical process of the **SYSTEM** and the **ASSOCIATED SERVICE** at the moment when the **ELECTRONIC DOCUMENT** is being generated.

6.1.4. **ELECTRONIC DOCUMENT** shall be signed by the **SYSTEM USER** with an **ELECTRONIC SIGNATURE** generated with the use of valid **TOKEN** by way of acceding it to the **ELECTRONIC DOCUMENT**.

6.1.5. The legal consequences provided for the **ELECTRONIC DOCUMENT** shall occur only upon receipt of successful result of **SIMPLE ELECTRONIC SIGNATURE** check-up of the relevant **ELECTRONIC DOCUMENT**.

6.1.6. **ELECTRONIC DOCUMENT** without an **ELECTRONIC SIGNATURE** or being in a format not meeting the requirements hereof, shall not be regarded as the **ELECTRONIC DOCUMENT** under the **SYSTEM** in accordance herewith.

6.2 Use of the Simple Electronic Signature

6.2.1 **ELECTRONIC DOCUMENT** shall be deemed signed by the **SYSTEM PARTICIPANT** and **the SYSTEM PARTICIPANT** shall be responsible for such signature, if the **ELECTRONIC DOCUMENT** contains **SIMPLE ELECTRONIC SIGNATURE** of the **SYSTEM USER,** whose **USER ACCOUNT** contains data on company name of the respective **SYSTEM PARTICIPANT**.

6.3 Use of ENHANCED ELECTRONIC SIGNATURE

6.3.1 An **ELECTRONIC DOCUMENT** shall be deemed signed by a **SYSTEM PARTICIPANT** and a **SYSTEM PARTICIPANT** shall be liable for such signing, if an **ELECTRONIC DOCUMENT** contains an **ENHANCED ELECTRONIC SIGNATURE** of a **SYSTEM USER,** whose **USER ACCOUNT** contains data on company name of the respective **SYSTEM PARTICIPANT.**

6.4 Use of SIMPLE ELECTRONIC SIGNATURE combined with additional data protection tools.

6.4.1. An **ELECTRONIC DOCUMENT** shall be deemed signed by a **SYSTEM PARTICIPANT** with the use of additional data protection tools and a **SYSTEM PARTICIPANT** shall be liable for such signing, if an **ELECTRONIC DOCUMENT** contains an **SIMPLE ELECTRONIC SIGNATURE** of a **SYSTEM USER,** whose **USER ACCOUNT** contains data on company name

of the respective **SYSTEM PARTICIPANT** and application of additional data security tools has been agreed with an **OPERATOR**.

6.5 Use of Electronic Document

6.5.1. Information in electronic format used by the **SYSTEM PARTICIPANT** to generate an **ELECTRONIC DOCUMENT** in accordance with these **RULES** and the contractual relations between **SYSTEM PARTICIPANTS**, shall be considered an **ELECTRONIC DOCUMENT** equal to a paper document signed with a manual signature provided that the following conditions are met simultaneously:

6.5.1.1 **ELECTRONIC SIGNATURE** in the **ELECTRONIC DOCUMENT** has been verified by checking validity of the **TOKEN** using technical process of the **SYSTEM**;

6.5.1.2. **ELECTRONIC SIGNATURE** is applied in the relations regulated with these **RULES,** rules of the **ASSOCIATED SERVICES**, and supplementary agreements signed between the **SYSTEM OPERATOR** and the **SYSTEM PARTICIPANTS;**

6.5.1.3. **ELECTRONIC DOCUMENT** is registered in the order provided for by clause 7.5 hereof.

7. Electronic document management arrangement procedure

7.1 Electronic Document Management may include:

7.1.1 Generation of **ELECTRONIC DOCUMENT**;

7.1.2 Sending and receiving of **ELECTRONIC DOCUMENT**;

7.1.3 Verification of **ELECTRONIC DOCUMENT**;

7.1.4 Recording of **ELECTRONIC DOCUMENT**;

7.1.5 Storage of **ELECTRONIC DOCUMENT** (**ELECTRONIC DOCUMENT** filing).

7.2 Generation of Electronic Document

7.2.1 **ELECTRONIC DOCUMENT** shall be generated in the following order:

7.2.1.1 Generation of **ELECTRONIC DOCUMENT** in the format established for this **ELECTRONIC DOCUMENT**;

7.2.1.2 Attachment of an **ELECTRONIC SIGNATURE** generated with the use of a **TOKEN** to the **ELECTRONIC MESSAGE**.

7.3 Sending and receipt of an Electronic Document

7.3.1 **ELECTRONIC DOCUMENT** shall be considered coming from an **ELECTRONIC DOCUMENT SENDER** in case the **ELECTRONIC DOCUMENT** was sent:

7.3.1.1 By **ELECTRONIC DOCUMENT SENDER**;

7.3.1.2 On behalf of the **ELECTRONIC DOCUMENT SENDER** using an automatic process launched by the **SENDER,** which forms a part of software tools of the **SYSTEM CLIENT, SYSTEM OPERATOR** or by **ORGANIZER OF ASSOCIATED SERVICE,** and is applied in accordance with the **SYSTEM RULES**.

7.3.2 **ELECTRONIC DOCUMENT** shall not be deemed coming from a **SENDER OF ELECTRONIC DOCUMENT** if:

7.3.2.1 **RECIPIENT OF ELECTRONIC DOCUMENT** knew or must have known, including following the results of **ELECTRONIC DOCUMENT** checkup, that the **ELECTRONIC DOCUMENT** does not come from **ELECTRONIC DOCUMENT SENDER**;

7.3.2.2 **RECIPIENT OF ELECTRONIC DOCUMENT** knew or must have known, including following the results of **ELECTRONIC DOCUMENT** checkup, that the received **ELECTRONIC DOCUMENT** was corrupted.

7.3.3 Special aspects of sending, transmission and receipt of the **ELECTRONIC DOCUMENT** may be determined by these **RULES,** the rules of the **ASSOCIATED SERVICES**, and supplementary agreements signed between **SYSTEM PARTICIPANTS.**

7.4 Electronic Document verification procedure

7.4.1 **ELECTRONIC DOCUMENT** verification procedure includes:

7.4.1.1 Review of the **ELECTRONIC DOCUMENT** by the **ASSOCIATED SERVICE** for compliance with the format set for it in accordance with the technical process of the **ASSOCIATED SERVICE**;

7.4.1.2 Verification of the attached **TOKEN**;

7.4.2 Attached **TOKEN** verification technology includes:

7.4.2.1 **ASSOCIATED SERVICE** performs verification procedure by applying to **TOKEN CONTROL INTERFACE** according to the process described in this section.

7.4.2.2 Verification of **TOKEN** used to generate **ELECTRONIC SIGNATURE** shall be performed by transferring of **TOKEN** by the **ASSOCIATED SERVICE** to **TOKEN CONTROL INTERFACE**. **TOKEN CONTROL INTERFACE** provides the result of **TOKEN** checkup procedure.

7.4.2.3 Verification of **TOKEN** used to generate **ELECTRONIC SIGNATURE** shall be successful if the following conditions are satisfied simultaneously:

7.4.2.3.1 **TOKEN** data provided by the **ASSOCIATED SERVICE** match with the **TOKEN** data provided earlier by the **SYSTEM**;

7.4.2.3.2 A registered **USER** with a unique identifier in the **TOKEN** exists in the **SYSTEM** with **USER ACCOUNT** which is not locked out;

7.4.2.3.3 Verified **TOKEN** has not been compromised;

7.4.2.3.4 **TOKEN** is valid as at the moment of checkup procedure.

7.4.3 **ASSOCIATED SERVICE** takes a decision on further processing of **ELECTRONIC DOCUMENT** basing on the results of verification of **TOKEN** used for generation of **ELECTRONIC SIGNATURE**.

7.4.4 In case of positive result of **ELECTRONIC DOCUMENT** verification, such **ELECTRONIC DOCUMENT** shall be considered valid. Otherwise **ELECTRONIC DOCUMENT** shall be considered invalid and the **RECIPIENT OF ELECTRONIC DOCUMENT** will be able to send a respective notification thereof to the **ELECTRONIC DOCUMENT SENDER** using the **SYSTEM.**

7.5 Recording of Electronic Document

7.5.1 **ELECTRONIC DOCUMENT** is recorded by maintaining electronic record logs. This implies issues of software system procedures of filling data into electronic record logs, maintaining and administering them and data storage. Tools used to maintain electronic record log are part of the software used to organize **ELECTRONIC DOCUMENT MANAGEMENT**.

7.5.2 Special issues of recording **ELECTRONIC DOCUMENTS** in the **SYSTEM** are determined by the rules of the **ASSOCIATED SERVICES** as well as supplementary agreements entered between the **OPERATOR** and **SYSTEM PARTICIPANTS.**

7.5.3 **SYSTEM OPERATOR** and **SYSTEM PARTICIPANTS** shall ensure unauthorized access protection and unintentional deletion and/or corruption of recorded data, contained in **ELECTRONIC DOCUMENTS** record logs owned by them. Period for retaining record data shall not be less than 5 (Five) years.

7.6 Electronic Document Storage

7.6.1 All recorded **ELECTRONIC DOCUMENTS** shall be stored during the terms stipulated by these **RULES** or the rules of the **ASSOCIATED SERVICES**. **ELECTRONIC DOCUMENTS** shall be stored in electronic archives.

7.6.2 **ELECTRONIC DOCUMENTS** shall be stored in the same format in which they were generated, sent or received, unless otherwise provided by the rules of the **ASSOCIATED SERVICE** and supplementary agreements entered between **SYSTEM PARTICIPANTS**.

7.6.3 Storage of **ELECTRONIC DOCUMENTS** shall be accompanied with storing corresponding electronic record logs and the software ensuring operation with electronic record logs and verification of **ELECTRONIC SIGNATURE** of stored **ELECTRONIC DOCUMENTS**.

7.6.4 Obligation to store **ELECTRONIC DOCUMENTS** shall be placed upon **SYSTEM OPERATOR, ORGANIZER OF ASSOCIATED SERVICE** and in case it is provided for by supplementary agreements entered between **SYSTEM PARTICIPANTS,** other **SYSTEM PARTICIPANTS**.

7.6.5 Electronic archives shall be secured from unauthorized access and unintentional deletion and/or corruption of recorded data.

8. Authentication data or Token compromise

8.1 In case **AUTHENTICATION DATA** or **TOKEN** is compromised, **SYSTEM USER** shall promptly notify **ADMINISTRATOR** of **COMPROMISE** of **AUTHENTICATION DATA** or **TOKEN** using a method determined by a **CLIENT**.

8.2 **CLIENT** represented by the **ADMINISTRATOR** shall use **USER CONTROL INTERFACE** to lock out the **USER ACCOUNT** of the **SYSTEM USER, AUTHENTICATION DATA** or **TOKEN** of which were specified in the notification of data **COMPROMISE**.

8.3 Date and time of successful locking out of **USER ACCOUNT** by **ADMINISTRATOR** in the **USER CONTROL INTERFACE** shall be deemed to be date and time of **COMPROMISE** of **AUTHENTICATION DATA** or **TOKEN**.

8.4 After the **ADMINISTRATOR** has successfully locked out the **USER ACCOUNT**, the **OPERATOR** shall provide impossibility of successful **USER AUTHENTICATION** and successful verification of all unexpired **TOKENS** issued to the **USER**.

8.5 After the **ADMINISTRATOR** has successfully locked out the **USER ACCOUNT**, all unexpired **TOKENS** issued to the **USER** shall be deemed compromised and such information shall be recorded with the **SYSTEM LOG**.

8.6 **ELECTRONIC DOCUMENT** signed by the compromised **ELECTRONIC SIGNATURE** generated with the compromised **TOKEN** shall be deemed improper and shall not produce any legal consequences for the **ELECTRONIC DOCUMENT SENDER** or **RECIPIENT**.

9. Procedure for settlement of disputes resulting from Electronic Document Management in the System

9.1 Conflict situations resulting from Electronic Document Management in the System

9.1.1. **ELECTRONIC DOCUMENT MANAGEMENT** may cause conflict situations related to generation, transmission, receipt of **ELECTRONIC DOCUMENT** and the **ELECTRONIC SIGNATURE** used therein. These conflict situations may arise, namely, in the following cases:

9.1.1.1 **ELECTRONIC DOCUMENT** was not verified by means of checkup of an **ELECTRONIC SIGNATURE**;

9.1.1.2 The fact of generation of an **ELECTRONIC DOCUMENT** is disputed;

9.1.1.3 **TOKEN** validity is disputed;

9.1.1.4 Registration of the **SYSTEM USER** that signed **ELECTRONIC DOCUMENT** in the **SYSTEM** is disputed;

9.1.1.5 Application of the **SYSTEM PARTICIPANT** on **ELECTRONIC DOCUMENT** corruption;

9.1.1.6 The fact of sending and/or receipt of **ELECTRONIC DOCUMENT** is disputed;

9.1.1.7 Time of sending and/or receipt of **ELECTRONIC DOCUMENT** is disputed;

9.1.1.8 Match of copies of **ELECTRONIC DOCUMENTS** and/or an original and a copy of **ELECTRONIC DOCUMENTS** is disputed;

9.1.1.9 Other cases of conflict situations connected with operation of the **SYSTEM**.

9.2 Notification on a conflict situation

9.2.1 In case of a conflict situation an **ORGANIZER OF ASSOCIATED SERVICE** or a **CLIENT** considering their rights have been violated, shall not later than within 3 (Three) business days or other shorter period of time specified in the rules of **ORGANIZERS OF ASSOCIATED SERVICE** and in agreements signed between the **SYSTEM OPERATOR** and **ORGANIZERS OF ASSOCIATED SERVICES,** from the day, when, accordingly, the **ORGANIZER OF ASSOCIATED SERVICE** or the **CLIENT** became aware or should have become aware of the violation of their rights, send a notification of the conflict situation to the **SYSTEM OPERATOR** and in case of a conflict situation in the framework of the **ASSOCIATED SERVICE –** to the **ORGANIZER OF** this **ASSOCIATED SERVICE**.

9.2.2 Notification on assumed conflict situation shall contain information on the essence of conflict and the facts that according to the notifier attest to the existence of a conflict situation. Regardless of the form in which the notification has been made (written or **ELECTRONIC DOCUMENT**) notification shall contain details of **ELECTRONIC DOCUMENT**, surname, name, patronymic, contact number, fax, email address of a person or persons authorized to negotiate a settlement of the conflict situation. In case a conflict affects interests of several **SYSTEM PARTICIPANTS,** a notifier shall specify in the notification contact details of all **SYSTEM PARTICIPANTS** (or authorized persons – representatives of **SYSTEM PARTICIPANTS**) whose interests were affected in this conflict situation.

9.2.3 Notification of a conflict situation shall be executed and sent in the form of an **ELECTRONIC DOCUMENT**, and in case it is impossible or not stipulated by the rules of **ORGANIZER OF ASSOCIATED SERVICE**, it shall be executed in the written form and sent by courier or using another method ensuring confirmation of receipt of correspondence by the recipient, with a fax or email message sent at the same time. A party receiving a notification shall immediately, but not later than during the next business day (or within another shorter period of time specified in the rules of **ASSOCIATED SERVICE** as well as in the agreements signed between **SYSTEM OPERATOR** and **ORGANIZERS OF ASSOCIATED SERVICE**) check existence of facts attesting to the occurrence of a conflict and provide a notifier with the information about the results of a check-up and, if necessary, with the measures taken to solve the conflict.

9.2.4 If necessary, in case of a conflict between the **CLIENTS, ORGANIZER OF ASSOCIATED SERVICE** shall at the written request of the **CLIENT** being in the dispute provide him with a confirmation of participation of disputing **CLIENTS** in the **ASSOCIATED SERVICE** and a

certified extract from a **SYSTEM LOG OF ASSOCIATED SERVICE** containing events registered with the **ASSOCIATED SERVICE** and relating to the subject of a dispute, in case a **CLIENT** provides reasonable grounds of its necessity for dispute resolution.

9.3 Dispute resolution in the due course

9.3.1 Conflict situation shall be deemed resolved in the course of business in case notifier is satisfied with the information provided by the **CLIENT** that have received the notification. In case a notifier is not satisfied with the information provided by the **CLIENT** that have received the notification, a technical commission shall be composed to deal with the conflict situation.

9.4 Technical commission, its members

9.4.1 Not later than on the day following the day when the **SYSTEM OPERATOR,** the **ORGANIZER OF ASSOCIATED SERVICE,** have made a decision on a technical commission, or not later that on the sixth day after receipt of notification of a conflict situation, in case such conflict has not been resolved in the due course, a technical commission shall be composed by the **SYSTEM OPERATOR** and the **ORGANIZER OF ASSOCIATED SERVICE.**

9.4.2 If the **CLIENTS** being parts of the conflict do not agree otherwise, dispute committee shall include an equal number, but not less than one authorized representative from each of the conflicting parties and a representative of the **SYSTEM OPERATOR** and, as agreed by the parties, a representative of an **ORGANIZER OF ASSOCIATED SERVICE**. In case of participation of a representative of the **SYSTEM OPERATOR,** technical commission shall operate at the location of the **SYSTEM OPERATOR**.

9.4.3 Technical commission shall be composed of specialists among employees of the technical and information security departments of the parties.

9.4.4 The right to stand for a relevant party and the **SYSTEM OPERATOR,** the **ORGANIZER OF ASSOCIATED SERVICE** shall be confirmed by the power of attorney issued to each representative for a period of commission operation.

9.4.5 On either party initiative, nonvoting independent experts with relevant knowledge in the sphere of data protection and computer information systems may be involved. A party attracting independent experts shall do this at its own expense.

9.4.6 Technical commission shall operate at the location of the **SYSTEM OPERATOR** or the **ORGANIZER OF ASSOCIATED SERVICE**.

9.5 Competence and powers of the technical commission

9.5.1 Upon solving a conflict situation a technical commission shall establish technical presence or absence of actual facts that indicate the fact and time of execution and/or sending of the **ELECTRONIC DOCUMENT**, its authenticity, the fact it was signed by a **SIMPLE ELECTRONIC SIGNATURE,** and if a sent and received **ELECTRONIC DOCUMENTS** are identical.

9.5.2 The commission shall have a right to consider any other technical issues necessary, according to the commission, to clarify the reasons and consequences of the conflict situation.

9.5.3 Commission shall not have the right to form a legal evaluation or any evaluation of other kind regarding the facts established thereby.

9.5.4 To perform necessary checking and documenting of data used thereupon, special software provided by the **SYSTEM OPERATOR** or the **ORGANIZER OF ASSOCIATED SERVICE** shall be applied.

9.6 Minutes of the technical commission

9.6.1 All measures taken by the commission to identify actual circumstances as well as conclusions made by the commission shall be recorded in the **MINUTES** of the technical commission (hereinafter referred to as the "**MINUTES**"). **MINUTES** shall contain the following data:

9.6.1.1 Members of the commission stating the qualification of each member;

9.6.1.2 Summary of the conflict;

9.6.1.3 Measures taken to find out the reasons and consequences of the conflict situation, including information regarding date, time and place where the measures were taken;

9.6.1.4 Conclusions made by the commission after all taken measures;

9.6.1.5 Signatures of all commission members.

9.6.2 In case opinion of a commission member (or members) concerning order, methods, aims of taken measures differs from the opinion of the majority of commission members, a respective record shall be made in the **MINUTES,** signed by a commission member (or members) whose special opinion is reflected by a respective record.

9.6.3 **MINUTES** shall be executed in one original paper copy stored with the **SYSTEM OPERATOR** or **ORGANIZER OF ASSOCIATED SERVICE**. At the request of any of the conflicting parties or any of the members of the technical commission, a copy of **MINUTES** signed by the **SYSTEM OPERATOR** or **ORGANIZER OF ASSOCIATED SERVICE** shall be transferred to them.

9.7 Report on technical commission operation

9.7.1 Following the results of work performed by the technical commission, a **REPORT** shall be executed to include a summary of conclusions made by the technical commission (hereinafter referred as the "**REPORT**"). In addition to conclusions, the **REPORT** shall contain the following data:

9.7.1.1 Composition of technical commission;

9.7.1.2 Date and time of the **REPORT**;

9.7.1.3 Starting date and time and duration of the commission work;

9.7.1.4 Short list of measures taken by the commission;

9.7.1.5 Conclusions made by the commission in the result of taken measures;

9.7.1.6 Signatures of commission members;

9.7.1.7 Reference to a special opinion of a member (or members) if any.

9.7.2 **REPORT** shall be made in a number of copies so that each conflicting party and **SYSTEM OPERATOR** or **ORGANIZER OF ASSOCIATED SERVICE** has one original copy of a **REPORT**. At the request of commission member it will be possible to receive a copy of a **REPORT** signed by **SYSTEM OPERATOR** or **ORGANIZER OF ASSOCIATED SERVICE**.

9.7.3 A special opinion of a dissenting member (or members) may be attached to the **REPORT**. Such opinion shall be made in any format in the same amount of original copies as the **REPORT** and shall constitute an attachment to the **REPORT**.

9.7.4 **REPORT** on the results of the work of technical commission shall be sent by the **SYSTEM OPERATOR** or **ORGANIZER OF ASSOCIATED SERVICE** to the conflicting parties with

special delivery or another method of dispatch providing acknowledgement of receipt of the correspondence by a recipient.

9.8 Complaint procedure

9.8.1 If a conflict situation is not regulated in the result of work of technical commission or otherwise, in case the **PARTICIPANT** considers that his rights were violated upon **ELECTRONIC DOCUMENT MANAGEMENT** under the **SYSTEM** or the **ASSOCIATED SERVICE,** he shall send a complaint to the party that, in his opinion, violated his rights.

9.8.2 A complaint shall contain:

9.8.2.1 Requirement of the **SYSTEM PARTICIPANT**;

9.8.2.2 Complaint amount and calculation (in case a complaint shall be estimated in monetary value);

9.8.2.3 Facts constituting grounds for the requirements and the evidences confirming them with a reference to legislative regulations and/ or internal regulatory documents;

9.8.2.4 Data on operation of the technical commission and, in case technical commission was working in relation with the conflict situation, copies of documents used in the process of work irrespective of conclusions made by the commission, agreement or disagreement of claimant with these conclusions; – other significant documents according to the claimant opinion;

9.8.2.5 List of documents attached to the complaint and other evidences and facts necessary for dispute resolution.

9.8.3 Complaint and all attached documents shall be sent with special delivery or another method of dispatch providing acknowledgement of receipt of the correspondence by a recipient.

9.8.4 The party receiving a claim shall not later than within 14 (Fourteen) business days settle it or provide its reasons for refusal in settling the claim. Default to provide an answer to the claim within a specified time shall constitute a violation of complaint procedure established by these **RULES** and may be considered by a person that sent such complaint as the refusal to settle a claim.

9.9 Dispute resolution in the Arbitral court

9.9.1 All disputes and disagreements between **SYSTEM PARTICIPANTS** arising in the result of **ELECTRONIC DOCUMENT MANAGEMENT** in accordance herewith and with application, breach, construing hereof, invalidating of these **RULES** or a part of them, in case a complaint was not satisfied in the terms established hereby, shall be resolved in the Arbitral court for the Novosibirsk region in accordance with the existing legislation of the Russian Federation.

9.9.2 Decisions of the Arbitral court shall be binding upon the parties. The decision of the Arbitral court, which has not been executed in time, shall be enforceable in accordance with the legislation of the Russian Federation.

10. Notification on amending these Rules

10.1 Amendments to these **RULES** and **APPENDIXES** thereto shall be communicated to **SYSTEM PARTICIPANTS** by **SYSTEM OPERATOR** by means of notification sent not less than 14 (fourteen) calendar days prior to entry of such amendments into force. Notification shall be performed by placing the respective data in the informative part of the **SYSTEM** in the Internet at the following address http://cft.group/company-group/contracts/.

10.2 These **RULES** shall be displayed in the informative part of the **SYSTEM** in the Internet at the address http://cft.group/company-group/contracts/.

APPENDIX N 1 TO
the RULES OF ELECTRONIC
DOCUMENT MANAGEMENT
OF CFT ID CORPORATE
INFORMATION SYSTEM

Agreement of accession to the "CFT ID" System

Novosibirsk ____ _____20__

_____, represented by_____, acting on the basis of_____, hereinafter referred to as "the Operator of the System", on the one side, and_____ (full name of the legal entity, full name, position and document on the basis of which he is acting/ full name of the individual), hereinafter referred to as "the System Participant" on the other side, hereby have concluded this Agreement of accession to the "CFT ID" System as follows:

1. The Subject of the Agreement is the accession of the System Participant to the Rules of the "CFT ID" System (hereinafter - "the Rules") which are available on the Internet at http://cft.group/company-group/contracts/, in the status of the _____.
2. The Rules of the "CFT ID" System are applied to the Operator of the System, the Users of the System, other System Participants only within the framework of their participation in the Associated services: _____.
3. This Agreement becomes effective from the date of its signing by the Parties and remains in effect until it is terminated on the grounds provided by the Rules, the Agreement and the current legislation.
4. Each Party is entitled to unilateral termination of this Agreement by the prior written notification sent to the other Party not later than three months prior to termination date.
5. By accessing to the Rules the System Participant accepts all the terms and conditions entirely in the manner prescribed by article 428 of the Civil Code of the Russian Federation and undertakes to fulfill them as well as accepts that receipt of the electronic document signed in accordance with this Rules by the electronic signature of the System Participant is legally equivalent to the receipt of the paper document certified by handwritten signatures of the System Participant /authorized persons of the System Participant and the stamp imprint of the System Participant. Obligations stated by this paragraph are valid provided that the Electronic Signature is created using the technologies of the System.
6. Details and signatures of the Parties.

The Operator of the System:	The System Participant:
_____ (_____)	_____ (_____)
Stamp	

APPENDIX 2 TO
the RULES OF ELECTRONIC
DOCUMENT MANAGEMENT
OF CFT ID CORPORATE
INFORMATION SYSTEM

List of Electronic Documents for operation in the Personal Area and User Control Interface

1. Upon operating in the **PERSONAL AREA** and **USER CONTROL INTERFACE,** the **USER** exchanges **ELECTRONIC DOCUMENTS** with the **SYSTEM OPERATOR** in accordance with the procedure of **ELECTRONIC DOCUMENT MANAGEMENT** described in the **RULES OF THE CFT ID SYSTEM.**

2. The following requests may be created upon working in the **PERSONAL AREA** and **USER CONTROL INTERFACE**:

2.1. **PERSONAL AREA** allows to exchange the following types of information signed with the **ELECTRONIC SIGNATURE**:

- Request for change of **IDENTIFICATION DATA**;
- Request for change of **AUTHENTICATION DATA**.

2.2. **USER CONTROL INTERFACE** allows for exchange with the following types of information signed with the **ELECTRONIC SIGNATURE**:

- Request for registration of the **USER**;
- Request for modification of **IDENTIFICATION DATA**;
- Request for modification of registration confirmation method;
- Request for modification of **AUTHENTICATION** method;
- Request for resending of email with a **LOGIN**;
- Request for resending of SMS message with a **LOGIN**;
- Request for locking of a **USER ACCOUNT**;
- Request for unlocking of a **USER ACCOUNT**.

APPENDIX N 3 TO
the RULES OF ELECTRONIC
DOCUMENT MANAGEMENT
OF CFT ID CORPORATE
INFORMATION SYSTEM

APPLICATION FOR REGISTRATION OF THE EMPLOYEE OF THE CLIENT AS THE ADMINISTRATOR (FORM)

(full name of the **SYSTEM CLIENT** (hereinafter- the **"CLIENT"**) represented by the authorized person of the **CLIENT** (position, full name) acting on the basis of (document confirming his powers) is hereby requesting to register the **EMPLOYEE OF THE CLIENT** as the **"ADMINISTRATOR"** within the framework of the **"CFT ID" SYSTEM:**

Full name	Olga Ivanovna Ivanova
E-mail (personal)	O.Ivanova@interbank.ru
Mobile telephone number (personal)	+79131232112
Confirmation method	☐ e-mail ; ☐ mobile telephone number

I hereby confirm that I am familiarized with the rules of electronic document interchange of the **"CFT ID" SYSTEM**:

✍ _____ _____

Signature of the employee *Full name*

AUTHORIZED PERSON OF THE CLIENT:

✍ _____ _____

Signature *Full name*

Place for seal

Date: _____ _____ 20 __

APPENDIX N 4 TO
the RULES OF ELECTRONIC
DOCUMENT MANAGEMENT
OF CFT ID CORPORATE
INFORMATION SYSTEM

APPLICATION FOR REGISTRATION OF THE EMPLOYEE/ THE EMPLOYEES OF THE CLIENT (FORM)

(full name of the **SYSTEM CLIENT (**hereinafter- the **"CLIENT"**) represented by the authorized person of the **CLIENT** (position, full name) acting on the basis of (document confirming his powers) is hereby requesting to register the following **EMPLOYEE/ EMPLOYEES OF THE CLIENT** within the framework of the **"CFT ID" SYSTEM:**

Full name	Position	Mobile telephone number (personal)	E-mail (personal)	Confirmation method
Ivan Ivanovich Ivanov	Accountant	+79131231221		☐e-mail; ☐mobile phone

AUTHORISED PERSON OF THE CLIENT:

_____ _____✍

Position *Signature* *Full name*

Place for seal

Date: _____ _____ 20 __

APPENDIX N 5
TO
the RULES OF ELECTRONIC DOCUMENT MANAGEMENT OF CFT ID CORPORATE INFORMATION SYSTEM

APPLICATION FOR AMENDING SYSTEM USER ACCOUNT (FORM)

(full name of the **SYSTEM CLIENT (**hereinafter- the **"CLIENT"**) represented by the authorized person of the **CLIENT** (position, full name) acting on the basis of (document confirming his powers) is hereby requesting to amend USER ACCOUNT within the framework of the **"CFT ID" SYSTEM:**

USER data:

Full name	Olga Ivanovna Ivanova
E-mail (personal)	O.Ivanova@interbank.ru
Mobile telephone number (personal)	+79131232112
Confirmation method	☐ e-mail ; ☐ mobile phone

Amended USED data:

Full name	
E-mail (personal)	
Mobile telephone number (personal)	
Confirmation method	☐ e-mail ; ☐ mobile phone

AUTHORISED PERSON OF THE CLIENT:

_____ _____✍

Position *Signature* *Full name*

Place for seal

Date: _____ _____ 20 __

APPENDIX N 6 TO
the RULES OF ELECTRONIC
DOCUMENT MANAGEMENT
OF CFT ID CORPORATE
INFORMATION SYSTEM

APPLICATION FOR LOCKING USER ACCOUNT / USER ACCOUNTS (FORM)

(full name of the **SYSTEM CLIENT** (hereinafter- the **"CLIENT"**) represented by the authorized person of the **CLIENT** (position, full name) acting on the basis of (document confirming his powers) is hereby requesting to lock the **USER ACCOUNT / USER ACCOUNTS** of the below listed **USERS** within the framework of the **"CFT ID" SYSTEM**:

Full name	Position	Personal phone number	E-mail (personal)
Ivan Ivanovich Ivanov	Accountant	+79131231221	

AUTHORISED PERSON OF THE CLIENT:

_____ _____✍

Position *Signature* *Full name*
Place for seal

Date: _____ _____ 20 __

APPENDIX No.7 TO THE RULES OF ELECTRONIC DOCUMENT MANAGEMENT OF CFT ID CORPORATE INFORMATION SYSTEM

APPLICATION FOR UNLOCKING THE USER ACCOUNT / USER ACCOUNTS (FORM)

(Full name of the **CLIENT OF THE SYSTEM** (hereinafter – the "**CLIENT**") represented by the authorized person of the **CLIENT** (position, full name), acting on the basis of (document confirming the powers), is hereby requesting to unlock the **USER ACCOUNT** / **USER ACCOUNTS** of the below listed **USERS** within the framework of the **"CFT ID" SYSTEM**:

Full name	Position	Mobile Phone No. (personal)	E-mail (personal)
Ivan Ivanovich Ivanov	Accountant	+79131231221	

AUTHORIZED PERSON OF THE CLIENT:

_____ _____ ✍

Position *Signature* *Full name*

Seal

Date: _____ _____ 20 __

APPENDIX No. 8 TO THE RULES OF ELECTRONIC DOCUMENT MANAGEMENT OF CFT ID CORPORATE INFORMATION SYSTEM

QUESSTIONNAIRY (FORM)

(Full name of the **SYSTEM CLIENT** (hereinafter – the "**CLIENT"**) represented by the authorized person of the **CLIENT** (position, full name), acting on the basis of (document confirming the powers), is hereby providing data for implementation of required additional security measures by the **CLIENT** within the framework of the **"CFT ID" SYSTEM**:

Table 1 – Parameters for Secure Data Exchange

Parameter	CLIENT	SYSTEM
VPN Gateway Information		
VPN Gateway Version		
Peer IP address		
APP LAN		
Private LAN		
ISAKMP		
encryption		
hash		
D-H group		
RestrictAuthenticationTo		
lifetime (sec)		
IPSec		
protocol		
encryption type		
hash		
pfs		
lifetime (sec)		

Upon implementation of secure information exchange using S-Terra complex, the **CLIENT** shall:

- Ensure support (operation capacity) of secure information exchange on its side in strict compliance with parameters specified in the Questionnaire;
- Send a new Questionnaire for reconfiguration of secure information exchange in case of any necessity to change parameters of Table 1;
- Ensure timely update of crypto keys and notification for reconfiguration of secure information exchange upon expiration of their validity period or compromise;
- Ensure measures against unauthorized access to secure information exchange (including S-Terra complex, crypto keys) on the **CLIENT** side.

AUTHORIZED PERSON OF THE CLIENT:

_____ _____ ✍

Position *Signature* *Full name*

Seal

Date: _____ _____ 20 __