Додаток 3 до Договору на приєднання до Публічної пропозиції за тарифним пакетом «____» №___ від __ _____ 20__ р.

ІНСТРУКЦІЯ ПРО ПОРЯДОК ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КЛЮЧОВОЇ ІНФОРМАЦІЇ
INSTRUCTIONS ON THE PROTECTION OF KEY INFORMATION

1. Персональний ключ ЕП та пароль доступу до нього є найбільш критичними даними з точки зору безпечної роботи користувача в системі.
Персональні ключі ЕП можуть зберігатися на рухомому носії інформації (дискеті, DVD/CD-диску, USB-накопичувачу). Зберігання (у т.ч. тимчасове) персональних ключів ЕП на жорсткому диску комп'ютера не припустимо.

1. Personal ES key signature and access password to it are the most critical data in terms of the safety of the user in the System.
Personal ES keys can be stored on a mobile information media (floppy, DVD / CD-ROM, USB-drives). Storage (including temporary) personal ES keys on the hard disk is not acceptable.

2. Носій ключової інформації (рухомий носій інформації, що містить ключ ЕП) повинен зберігатися під особистим контролем його власника – користувача Системи, який забезпечує унеможливлення доступу до нього інших осіб. Передавання носія ключової інформації та/або розголошення паролю доступу до персонального ключа ЕП іншим особам, у тому числі співробітникам Банку заборонено.

2. Key information carrier (mobile information carrier that contains the ES key) should be kept under the personal supervision of the owner - user of the System who must prevent the access to it of other persons. Transferring of the key information carrier and/or disclosure access password to ES key to other persons, including employees of the Bank is prohibited.

3. Носій ключової інформації повинен використовуватись тільки під час роботи в системі. Не допустимо залишати носій ключової інформації приєднаним до персонального комп'ютера, коли робота в системі призупинена або не проводиться.
Для персональних ключів ЕП, що зберігаються на рухомому носії, обов'язкове використання SMS-аутентифікації (додатковий пароль для входу в систему, що надходить за допомогою SMS-повідомлення)..

3. Key information carrier shall be applied only during the work in the System. It is not allowed to leave the key information carrier attached to a personal computer when the work in the System is suspended.
For personal ES keys that are stored on a mobile carrier it is obligatory to use SMS authentication (additional password for logging in the System, entering via SMS).

4. Термін дії персонального ключа ЕП визначається Банком самостійно та зазначається в Додатку 2 до Договору. У разі нездійснення своєчасної зміни персонального ключа ЕП доступ користувача до системи буде заблоковано. Користувач має право самостійно виконувати позапланову зміну персонального ключа ЕП. Після активації нового персонального ключа ЕП в Системі або у разі відключення від Системи користувач повинен знищити неактуальний ключ ЕП, що міститься на носії ключової інформації.

4. Validity duration of personal ES key shall be determined by the Bank and specified in Exhibition 2 to the Agreement. In case of failure to timely change personal ES key user access to the system will be blocked. The user has the right independently to perform unscheduled change of personal ES key. After activating of the new personal ES key in the System or in case of disconnection from the System user must destroy outdated ES key kept on the key information carrier.

5. Пароль доступу до персонального ключа ЕП не повинен зберігатись у відкритому вигляді (наприклад, записаним на паперовому носії тощо) та використовуватись для доступу до інших систем та сервісів. Персональна відповідальність за збереження паролю доступу до персонального ключа ЕП та захист носія ключової інформації від використання іншою особою покладається на користувача.

5. Access password to the personal ES key shall not be stored in unclosed view (for example, written on paper, etc.) and used to access to other systems and services. Personal responsibility for maintaining access password to the personal ES key and protection of key information carrier from the use of other persons is conferred on the user.

6. Користувач зобов'язаний не рідше одного разу на місяць змінювати пароль доступу до персонального ключа ЕП, що повинен містити щонайменше 6 символів та складатися з цифр, літер верхнього та нижнього регістрів, спеціальних символів. При виборі паролю не допускається використання комбінацій, що легко вгадуються, наприклад, імен, дат народження, телефонних номерів тощо.

6. User must at least once a month to change the access password to personal ES key digital signature, which must contain at least 6 characters and be consisted of numbers, upper and lower case letters, special characters. At choosing a password is not allowed to use combinations that are easily guessed, such as names, birth dates, phone numbers etc.

7. Необхідно забезпечити обов'язкову наявність на персональному комп'ютері, з якого здійснюється доступ до системи, наступного програмного забезпечення:
7.1. ліцензійного антивірусного програмного забезпечення. База даних вірусних сигнатур повинна оновлятись щоденно;
7.2. ліцензійного антишпигунського програмного забезпечення (Antispyware);
7.3. мережевого екрану (Firewall, брандмаеру), який повинен бути налаштований таким чином, щоб максимально обмежити вихідний та вхідний мережевий трафік.
Антивірусне та антишпигунське програмне забезпечення повинне бути налаштоване для моніторингу всіх подій та періодичного сканування інформації, що зберігається на

7. The computer connected to the System must be obligatory equipped with the following software:
7.1. licensed antivirus software. The database of virus signatures must be daily updated;
7.2. licensed antispy software (Antispyware);
7.3. network screen (Firewall, Brandmayer), which should be set so as to maximally restrict the incoming and outgoing network traffic.
Antivirus and antispy software should be configured in such a way as to monitor all events and periodically to scan the information stored on the hard disk of the personal computer, from which the access to the System is done.

жорсткому диску персонального комп'ютера, з якого здійснюється доступ до системи.

8. Забороняється встановлювати на персональний комп'ютер, з якого здійснюється доступ до системи, програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо). Не рекомендується використовувати персональний комп'ютер, з якого здійснюється доступ до системи, для доступу до ненадійних (незнайомих) інтернет-ресурсів.

8. It is forbidden to install on the personal computer with access to the System the software from unreliable sources (public library of software programs, e-mail programs, etc.). It is not recommended to use a personal computer with an access to the System for access to unreliable (unknown) Internet resources.

9. Для поточної роботи в системі забороняється використання облікового запису користувача з правами «Адміністратор».

9. For the current operation in the System it is forbidden to use a user account with rights of "Administrator".

10. Під час підключення до веб-сайту Банка (https://ibank.unexbank.ua) користувачу необхідно переконатися у коректній автентифікації веб-сайту системи під час SSL-сесії.
Користувачу забороняється здійснювати доступ до системи через посилання, отримані засобами електронної пошти, або з неконтрольованих та ненадійних робочих місць (інтернет-кафе, готелі, офіси інших організацій тощо).

10. At connecting to the Bank's website (https://ibank.unexbank.ua) the user must ensure in proper authentication Website of the Systems during SSL-session.
The user is prohibited to link the System via messages received by e-mail, or uncontrolled and insecure working place (Internet cafes, hotels, offices, other organizations, etc.).

11. З метою встановлення обмеження переліку IP-адресів та/або IP-підмереж, з яких можливе підключення до системи, Клієнт може звернутися до Банку шляхом подання письмової заяви про встановлення зазначеного обмеження за підписом уповноважених осіб та відбитком печатки Клієнта (за наявності).

11. In order to establish limit of the IP-address list and/or IP-subnet from which the connection may be done to the System, the Client may request the Bank by submitting a written application on setting mentioned limit, signed by the authorized person and sealed by the Client (if available).

12. Якщо налаштування персонального комп'ютера, з якого здійснюється доступ до системи, здійснює інша особа, необхідно забезпечити контроль за всіма діями такої особи на персональному комп'ютері.

12. If the personal computer with access to the System is being set by another person it is necessary to secure control over all actions of such a person on a personal computer.

13. З метою заволодіння приватними даними Клієнта (персональний ключ ЕП та пароль доступу до нього) для їх подальшого незаконного використання зловмисники здійснюють фішингові або хакерські атаки.
Основні методи заволодіння ключовою інформацією:
– розсилання Клієнту підроблених електронних листів та адрес інтернет-сайтів, що маскуються під банківські, з пропозицією надати інформацію щодо приватних даних Клієнта/ його уповноважених осіб начебто для звірки;
– розповсюдження через електронні листи або інтернет-сайти програмного забезпечення із зловмисним кодом (програмним вірусом) для заволодіння приватними даними Клієнта/ його уповноважених осіб;
– несанкціоноване дистанційне управління персональним комп'ютером Клієнта шляхом віддаленого доступу.
При виконанні Клієнтом запропонованих дій або при виконанні стандартних дій входу до системи програмний вірус копіює персональний ключ ЕП та пароль доступу до нього, та передає цю інформацію зловмисникам.
Щоб запобігти несанкціонований доступ та заволодіння ключовою інформацією необхідно знати, що Банк не здійснює розсилку електронних листів з вимогою надіслати персональний ключ ЕП та/або пароль доступу до нього, не пропонує перейти за вказаною електронною адресою та не розповсюджує електронною поштою комп'ютерні програми.
Відповідальність за збереження конфіденційності персональних ключів ЕП покладається на Клієнта, як на єдиного власника таких ключів.
У разі отримання листів, програм чи будь-яких повідомлень засобами електронної пошти, що вимагають надіслання персональних ключів ЕП та/або введення паролю доступу до персонального ключа ЕП або інших дій, пов'язаних із несанкціонованим доступом до Системи, Клієнт зобов'язаний негайно повідомити Банк відповідно до умов Договору.
Рекомендується видаляти підозрілі повідомлення, що надійшли засобами електронної пошти, без їх відкриття. Користувач повинен запобігати відкриттю електронних листів від невідомих відправників з приєднаними файлами, що мають

13. For the purpose of taking possession of private Client's data (personal ES key and access password to it) for further illegal use, violators carry out fishing or hacking attacks.
Main methods of seizure of key information:
- mail-out of fake emails and addresses of Internet-sites concealed under bank ones with a request to provide information about the private data of the Client/ its authorized persons as if for a verification;
- Distribution through emails or internet-sites of software with a malicious code (software virus) for the acquisition of private Client's data or its authorized persons;
- Unauthorized remote control over personal computer by a distanced access.
At performing proposed actions or standard login program to the System the program virus copies personal ES key and access password to it, and passes this information to attackers.
In order to prevent unauthorized access and seizure of key information it is necessary to know that the Bank does not send emails with the requirement to send a personal ES key and/or access password to it, does not offer to go over to the specified e-mail or otherwise distribute software programs.
Responsibility for maintaining the confidentiality of personal ES keys shall be confer on the Client as the sole owner of the keys.
In case of receiving of letters, programs or any communications by means of electronic mail with a request to deliver personal ES keys and/or access password to personal ES keys or other actions related to unauthorized access to the system, the Client is obliged immediately notify a Bank under the terms of the Agreement.
It is recommended to delete suspected messages without opening them. The user must prevent opening electronic letters from unknown senders with attached files with name suffix *.exe, *.pif, *.vbs and other files.

розширення *.exe, *.pif, *.vbs та інші файли, що можуть бути виконані.

З Інструкцією ознайомлений та згоден нести відповідальність за її неналежне виконання:

__ _____ 20__ р. _____ _____
підпис П.І.Б.

М. П.

Read the instructions and agree to be responsible for its improper performance:

__ _____ 20__ _____ _____
Signature Name

Seal

Сторона 1. Банк		**Party 1. Bank**	
Назва Банку:	**АТ «ЮНЕКС БАНК»**	**Name:**	**JSC "UNEX BANK"**
Адреса реєстрації:	03040, Україна, м. Київ, вул. Васильківська, 14,	**Reg. address:**	14 Vasylkivska Street, Kyiv 03040 Ukraine
Тел./ факс:		**Phone / fax:**	
Код банку:	322539	**Bank Code:**	322539
Код ЄДРПОУ:	20023569	**USREOU Code:**	20023569
Міжнародний номер банківського рахунку (IBAN):	UA503000010000032003119701026	**IBAN:**	UA503000010000032003119701026
Відділення банку:		**Branch:**	
Адреса відділення банку:		**Address of the branch:**	
Тел./факс відділення:		**Phone / fax of the branch:**	
Посада:	_____	**Title:**	_____
_____	_____	_____	_____
(підпис)	(ПІБ)	(signature)	(Name)
М.П.		Seal	

Сторона 2. Клієнт	**Party 2. Client**
Назва:	**Name:**
Адреса реєстрації:	**Registration address:**
Тел./ факс:	**Phone/fax:**
Адреса для листування:	**Post address:**
Код ЄДРПОУ/ податковий номер:	**USREOU Code/ tax number:**
Міжнародний номер банківського рахунку (IBAN):	**IBAN:**
Посада: _____	**Title:** _____
_____ _____	_____ _____
(підпис) (ПІБ)	(signature) (Name)
М.П.	Seal
Другий примірник договору отримано _____ (підпис) /_____ / (ПІБ)	Copy #2 is received: _____ (signature) /_____ / (Name)