Додаток 4.1. *до Правил та загальних умов комплексного банківського обслуговування (Для корпоративного бізнесу)*

БАНК КЛІРИНГОВИЙ ДІМ

1. **Порядок використання секретних ключів** Секретні ключі — це сукупність записів, записаних оригінальним засобом на носії інформації (USB-токен, USB-флеш накопичувач, директорія на жорсткому диску комп'ютера) будь-якого формату та призначені для шифрування електронних фінансових повідомлень з метою забезпечення конфіденційності при передачі їх по відкритим каналам зв'язку.

2. Клієнт генерує секретні ключі самостійно під час реєстрації в Системі ("Інтернет- Банк") (далі – Система). Звіт про реєстрацію відкритого ключа Клієнта, створений під час реєстрації в системі, надсилається у Банк.

3. Клієнт призначає посадову особу, яка несе відповідальність за зберігання секретних ключів та вірність їх використання.

4. Відповідальність цього співробітника Клієнт закріплює документально та надає Банку відповідний документ.

5. У разі зміни відповідального співробітника Клієнт зобов'язаний згенерувати новий секретний ключ та надати в Банк відповідний документ.

6. Створення нового ключа клієнт здійснює самостійно, обов'язково погоджуючи свої дії з адміністратором Системи ("Інтернет-Банк") у Банку.

7. Носії інформації з секретними ключами Клієнт зобов'язаний зберігати у сейфах, крім випадків коли у ролі носія ключа використовується USB-токен.

8. Максимальні строки дії сертифікатів секретних ключів електронно-цифрового підпису Системи, в розрізі наступних груп ризику, залежить від використання суб'єктом господарювання додаткових сервісів безпеки **(підключення до сервісів безпеки здійснюється на підставі наданого Клієнтом клопотання про надання сервісу – з додатком 4.3.)**, а саме:

- **I рівень ризику – максимальний строк дії сертифікатів 6 місяців:**

- використання незахищених носіїв приватних електронних ключів (USB-накопичувачі, директорія на жорсткому диску комп'ютера).

- **II рівень ризику – максимальний строк дії сертифікатів 12 місяців:**

- використання захищених носіїв приватних електронних ключів (USB-токени).

- **III рівень ризику - максимальний строк дії сертифікатів 12 місяців (за умови одночасного використання двох сервісів безпеки з одноразовими паролями):**

- використання сервісу «багатофакторна автентифікація» (процедура встановлення автентичності користувача при вході до Системи за допомогою введення одноразового шестизначного паролю до спеціального додаткового поля, який направляється у вигляді SMS-повідомлення на вказаний клієнтом номер мобільного телефону і має обмежений термін дії -3 хв.);

- використання сервісу «підтвердження платіжних документів одноразовим паролем» (процедура введення одноразового шестизначного паролю на певні платежі від зазначеної клієнтом суми до спеціального додаткового поля, який направляється у вигляді SMS-повідомлення на вказаний клієнтом номер мобільного телефону і має обмежений термін дії -3 хв.).

- **IV рівень ризику – максимальний строк дії сертифікатів 24 місяця (за умови одночасного використання захищеного носія електронного ключа та двох сервісів безпеки з одноразовими паролями):**

- використання захищених носіїв приватних електронних ключів (USB-токени);

- використання сервісу «багатофакторна автентифікація» (процедура встановлення автентичності користувача при вході до Системи за допомогою введення одноразового шестизначного паролю до спеціального додаткового поля, який направляється у вигляді SMS-повідомлення на вказаний клієнтом номер мобільного телефону і має обмежений термін дії -3 хв.);

- використання сервісу «підтвердження платіжних документів одноразовим паролем» (процедура введення одноразового шестизначного паролю на певні платежі від зазначеної клієнтом суми до спеціального додаткового поля, який направляється у вигляді SMS-повідомлення на вказаний клієнтом номер мобільного телефону і має обмежений термін дії -3 хв.).

9. Банк здійснює контроль за зберіганням та використанням секретних ключів.

10. Якщо Клієнт порушив правила зберігання секретних ключів або втратив їх, то Банк має право призупинити електронне обслуговування Клієнта до ліквідації причин порушення правил зберігання та використання секретних ключів.

11. У випадку виявлення 3-х випадків порушень правил зберігання та використання ключових матеріалів Банк залишає за собою право перевести Клієнта з електронного обслуговування на звичайне (паперове).

КЛІЄНТ:

_____ _____ (_____)

Посада *М.П.* *П.І.Б.*