Додаток 2
до Публічної пропозиції АТ «КРИСТАЛБАНК»
на укладання договору комплексного банківського
обслуговування юридичних та самозайнятих осіб

Вимоги Банку та рекомендації Клієнту щодо безпечної роботи з системою «Клієнт-Банк»

1. Негайно інформуйте Банк до відділення, де Ви обслуговуєтесь, щодо нештатних ситуацій або підозри на порушення безпеки робочого місця Системи, якщо:

1. при отриманні SMS повідомлення про платіж, який Ви не виконували (у випадку підключення такої послуги);
2. при виявленні у виписці по Вашому рахунку платіжних операцій, яких Ви не виконували;
3. у Вас не працює Система з невідомих причин;
4. у випадку, навіть тимчасової втрати контролю над ключовими носіями, та існуванні вірогідності того, що з носія ключа ЕП може бути виготовлена копія;
5. при будь-якій підозрі, що ключ може бути скопійований;
6. у випадку несанкціонованого користування Системою, коли Ви, як керівник не контролювали таке використання, з інших комп'ютерів (публічних бібліотек, Інтернет - кафе або з комп'ютера, до якого мають доступ інші співробітники організації);

2. Рекомендації щодо роботи з ключовими носіями електронно-цифрового підпису:

1. перед генерацією ключа підготуйте носій інформації, на якому Ви будете зберігати ключ ЕП. Для цього:

- використовуйте окремий, спеціально виділений змінний носій, попередньо відформатований та перевірений на відсутність вірусів;

2. не використовуйте ключовий носій для інших цілей (копіювання та зберігання файлів будь-якої іншої інформації, окрім збереження ключа ЕП);
3. після генерації ключа ЕП уважно контролюйте місце збереження носія. Не робіть копію ключа ЕП;
4. ні в якому випадку не зберігайте ключ ЕП на жорсткому диску комп'ютера;
5. не передавайте нікому носій інформації з ключем ЕП та пароль до нього, включаючи працівників Вашого підприємства (організації);
6. підключайте ключовий носій з ЕП до комп'ютера лише на момент роботи з Системою, в усіх інших випадках, якщо Ви не працюєте в Системі, не залишайте ключовий носій підключеним до комп'ютера та зберігайте його в надійному, контрольованому місці;
7. при генерації нового ключа обов'язково змінюйте пароль доступу до нього, з дотриманням таких правил:

- пароль повинен бути комбінований з використанням великих та малих латинських літер, службових символів (!, -, ?, &, $ та інші) та цифр (1, 2, …9)

3. Завжди виконуйте перегенерацію (заміну) ключа ЕЦП у випадках:

1. виявлення вірусів на Вашому комп'ютері;
2. виявлення програм віддаленого доступу на Вашому комп'ютері;
3. виявлення змін у налаштуванні служб та засобів віддаленого управління Вашим комп'ютером;
4. звільнення або заміні уповноважених осіб Клієнта на підписання документів;

4. Рекомендації щодо користування персональним комп'ютером, на якому встановлено Систему:

1. обмежте доступ працівників до комп'ютера (тільки відповідальні за роботу в Системі), з якого виконуються платежі в Системі;

2. рекомендується для роботи в Системі використовувати окремий, призначений лише для роботи з цією системою комп'ютер;

3. використовуйте програмне забезпечення (надалі – ПЗ) отримане лише з достовірних джерел (ліцензійне ПЗ), відслідковуйте та своєчасно встановлюйте усі останні версії операційної системи, поновлення антивірусних баз, системного ПЗ, Web-браузера та віртуальної Java-машини;

4. встановлюйте та використовуйте Систему лише після того, як будете впевнені, що Ваш комп'ютер не заражений вірусами та на ньому відсутнє шкідливе ПЗ;

5. налаштовуйте систему антивірусного захисту на перевірку у режимі реального часу. Регулярно контролюйте поновлення антивірусного ПЗ;

6. використовуйте сервіси Системи, які запобігають шахрайським операціям з рахунками, наприклад: (SMS-Банкінг);

7. категорично не рекомендується установка програм для дистанційного управління (Microsoft Remote Assistant, Team Viewer, Radmin та ін.) на комп'ютері, на якому встановлена Система;

8. перевірити та виключити на комп'ютері, на якому встановлена Система, використання будь-яких служб віддаленого управління Вашим комп'ютером, наприклад: віддалений помічник, дистанційне управління робочим столом, служба терміналів, Telnet, віддалений реєстр та ін.;

9. категорично не рекомендується скачувати та встановлювати неперевірене ПЗ, відкривати неперевірені повідомлення та додатки до повідомлень (особливо від невідомих відправників);

10. встановіть персональний файрвол та налаштуйте його в максимально жорсткому режимі – на обмін лише з банківським сервером Системи;

11. постійно, перед початком роботи в Системі, тестуйте комп'ютер на відсутність вірусів та руйнівного ПЗ;

12. на комп'ютері не повинно бути облікових записів користувачів з пустими паролями. При створені паролю для облікового запису або ключа ЕЦП дотримуйтесь таких правил:

- пароль повинен бути комбінований з використанням великих та малих латинських літер, службових символів (!, -, ?, &, $ та інші) та цифр (1, 2, …9)

13. не рекомендується працювати під технологічними обліковими записами, наприклад: Адміністратор, а також під обліковими записами що мають права адміністратора.

5. Додаткові рекомендації:

1. регулярно контролюйте рух коштів та залишки на Ваших рахунках;

2. виконуйте прив'язку IP-адреси свого комп'ютера (у випадку використання статичної IP-адреси) до Системи.

!!! Пам'ятайте,

що лише своєчасне звернення до Банку дозволить прийняти оперативні заходи щодо попередження шахрайства та повернення коштів, які були нелегально списані з Вашого рахунку.

З рекомендаціями Банку, щодо безпечної роботи з Системою, ознайомлений і зобов'язуюсь їх виконувати.

Я розумію, що невиконання вищезазначених рекомендацій може потягти за собою несанкціоноване списання коштів з мого рахунку.