Правила дотримання персональних заходів безпеки при роботі з Комплексом електронного банкінгу
(згідно п.4.7. Правил обслуговування корпоративних клієнтів)

4.7.1. Для початку роботи в Комплексі електронного банкінгу введіть адресу сайту Комплексу в браузері: **https://ibank.tascombank.com.ua/**. Не використовуйте для переходу на сторінку Комплексу банерні посилання чи посилання отримані в електронних листах.

4.7.2. Перед початком роботи в Комплексі слід впевнитись, що Ви знаходитесь саме на сторінці Банку: **https://ibank.tascombank.com.ua/**. Обов'язково перевірте, щоб адреса починалася з **https**, де літера «**s**» вказує на ознаку захищеного з'єднання.

4.7.3. Ніколи не розголошуйте Ваші персональні дані, що Ви використовуєте для роботи в Комплексі (логін та пароль, OTP, дані щодо рахунків тощо), стороннім особам, в тому числі отримавши лист чи дзвінок від осіб, що представляються співробітниками Банку.

4.7.4. Не зберігайте Ваші авторизаційні дані (логін та пароль) на обладнанні (ПК, ноутбук, смартфон і т.п.) з якого здійснюється робота в Комплексі. Не зберігайте Ваші логін та пароль в будь-якому вигляді та місці, що можуть бути доступним стороннім особам (наприклад, записи на паперових носіях та у електронних текстових файлах).

4.7.5. Ніколи не зберігайте ЕЦП на смартфоні. Якщо для авторизації та підписання платежів у комплексі електронного банкінгу використовується ЕЦП, що було записано на звичайний Змінний носій (flash-usb), замість апаратного USB-токену, то ніколи не переміщайте дані ЕЦП зі Змінного носія (flash-usb) на ПК, ноутбук, смартфон тощо.

4.7.6. У випадку підозри що Ваші авторизаційні дані для доступу до Комплексу стали відомі стороннім особам, змініть пароль доступу до Комплексу та, у разі необхідності, зверніться до Банку щодо блокування доступу до Комплексу.

4.7.7. Категорично не рекомендується використання функцій «запам'ятовування пароля» веб-браузером чи іншим програмним забезпеченням, що встановлено на Вашому обладнанні, з якого здійснюється вхід до Комплексу. Це особливо важливо, коли ви використовуєте для зберігання ЕЦП звичайний Змінний носій (flash-usb), замість апаратного USB-токену.

4.7.8. Рекомендуємо Вам змінювати пароль доступу до Комплексу не рідше одного разу на три місяці. Також рекомендуємо при створенні паролю використовувати комбінації як мінімум з літер та цифр. Не рекомендуємо використовувати легкі для підбору паролі та паролі пов'язані з Вашими персональними даними чи даними Ваших близьких тощо.

4.7.9. Використовуйте на Вашому обладнанні, з якого здійснюється доступ до Комплексу, антивірусне програмне забезпечення. Також здійснюйте регулярне оновлення вірусних баз до антивірусного програмного забезпечення. Якщо на Вашому обладнанні виявлено будь-яке шкідливе програмне забезпечення, слід здійснити вхід до Комплексу з гарантовано незараженого обладнання та змінити пароль доступу до Комплексу.

4.7.10. Регулярно встановлюйте оновлення операційної системи Вашого обладнання, з якого здійснюється доступ до Комплексу, в тому числі встановлюйте оновлення безпеки операційної системи. Використовуйте ліцензійне програмне забезпечення.

4.7.11. Не рекомендуємо використовувати Комплекс на комп'ютерах, що встановлені у публічних місцях. Зауважте, що будь-яка особа, яка має безпосередній доступ до обладнання, з якого здійснюється доступ в Комплекс, може встановити на нього шкідливе програмне забезпечення з метою перехоплення ваших авторизаційних даних.

4.7.12. По закінченню роботи із Комплексом, обов'язково здійснюйте безпосередній вихід із Комплексу, натиснувши відповідну кнопку «Вийти».

4.7.13. Ніколи не залишайте після завершення роботи з Комплексом носій з ЕЦП вставленим у ПК.

4.7.14. При користуванні бездротовою мережею Wi-Fi, впевніться, що Ваша мережа захищена паролем. Уникайте використання Комплексу під час підключення до мереж Wi-Fi в публічних місцях.

4.7.15. Не відповідайте на листи з проханням вислати будь-які персональні данні, логін та пароль від Комплексу, або OTP. Банк ніколи не здійснює розсилку електронних листів, SMS чи інших повідомлень із вимогою уточнити чи надати Ваші конфіденційні дані.

4.7.16. У випадку виявлення фактів несанкціонованого переказу коштів з Ваших рахунків, просимо терміново повідомити про цей факт працівника Банку, або зателефонувати до Банку за номером: **0 800 503 580** або **044 393 25 90** (дзвінки з стаціонарних телефонів безкоштовні).