ЗАХОДИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Використовуйте на Робочому місці тільки ліцензоване програмне забезпечення.
2. Використовуйте на Робочому місці засоби антивірусного захисту та регулярно їх оновлюйте, використовуйте ліцензоване антишпигунське програмне забезпечення, а також міжмережеві екрани (фаєрволи).
3. Не здійснюйте тиражування та використання Системи/Системи онлайн-банкінгу «КРЕДОБАНК» та документації до неї для інших цілей, ніж це передбачено Правилами.
4. Забезпечуйте надійне збереження носія інформації з удосконаленим електронним підписом для Системи (Удосконалений ЕП для Системи)/ Удосконаленим електронним підписом з кваліфікованим сертифікатом (Удосконалений ЕП з кваліфікованим сертифікатом)/Кваліфікованим електронним підписом (Кваліфікований ЕП). Зберігайте носій інформації з Удосконаленим ЕП для Системи/ Удосконаленим ЕП з кваліфікованим сертифікатом/Кваліфікованим ЕП в умовах, що забезпечують його захист від несанкціонованого доступу неуповноважених третіх осіб, а також забезпечте доступність носія інформації з Удосконаленим ЕП для Системи/ Удосконаленим ЕП з кваліфікованим сертифікатом/Кваліфікованим ЕП виключно Користувачам та тільки під час роботи з Системою/ Системою онлайн-банкінгу «КРЕДОБАНК». Не допускайте передавання Користувачами носіїв інформації з Удосконаленим ЕП для Системи/ Удосконаленим ЕП з кваліфікованим сертифікатом/Кваліфікованим ЕП іншим особам. Носій інформації з Удосконаленим ЕП для Системи/ Удосконаленим ЕП з кваліфікованим сертифікатом/Кваліфікованим ЕП має бути доступний тільки Користувачу. Спосіб зберігання носія інформації з Удосконаленим ЕП для Системи/ Удосконаленим ЕП з кваліфікованим сертифікатом/Кваліфікованим ЕП повинен унеможливлювати доступ до них будь-яких інших осіб. Спосіб зберігання носіїв інформації з Удосконаленим ЕП для Системи має забезпечувати доступ до них Користувачу тільки в період їх використання під час роботи в Системі/Системі онлайн-банкінгу «КРЕДОБАНК».
5. Забезпечуйте збереження Одноразового коду таким чином, щоб виключити його використання будь-ким, крім Користувача, для якого Одноразовий код надісланий.
6. Забезпечуйте обмежений доступ до Робочого місця, на якому встановлено модуль Системи/Систему онлайн-банкінгу «КРЕДОБАНК» або з якого відбувається доступ до Системи/ Системи онлайн-банкінгу «КРЕДОБАНК», виключно належно уповноваженим Користувачам.
7. Забезпечуйте нерозголошення даних, що застосовуються для автентифікації Користувача в Системі/Системі онлайн-банкінгу «КРЕДОБАНК» (Логіни, паролі, Одноразові коди тощо), в тому числі конфіденційних відомостей про Особисті робочі ключі (пароль тощо), будь-яким іншим особам.
8. Не зберігайте Особисті робочі ключі, в тому числі паролі до них, на жорсткому диску Робочого місця.
9. Зберігайте Особисті робочі ключі виключно на переносних носіях інформації (USB-flash накопичувач, CD-диск тощо).
10. Не використовуйте Систему/Систему онлайн-банкінгу «КРЕДОБАНК» з Робочих місць в громадських місцях (Інтернет-кафе, бібліотеки тощо), а також з будь-якого іншого обладнання, налаштування та експлуатація яких знаходиться поза контролем Клієнта.
11. Забезпечуйте регулярну зміну паролів до Особистих робочих ключів.
12. Не використовуйте простих паролів до Особистих робочих ключів (до простих паролів прирівнюється, зокрема: ім’я, прізвище, дата народження Користувача, повторювання однакових знаків, використання знаків, які послідовно розміщені на клавіатурі тощо). Пароль потрібно регулярно змінювати і він повинен складатися не менше, ніж з 8 (восьми) знаків (цифри, літери тощо).
13. Для входу на WEB-сторінки Системи або Системи онлайн-банкінгу «КРЕДОБАНК» використовуйте лише адресу: https://ifobs.kredobank.com.ua або https://online.kredobank.com.ua/auth/login.
14. Для завантаження та встановлення на Мобільний пристрій відповідний мобільний застосунок Системи/Системи онлайн-банкінгу «КРЕДОБАНК» використовуйте лише офіційні магазини додатків (якщо відповідний пристрій працює на базі операційної системи iOS мобільний застосунок Системи/ Системи онлайн-банкінгу «КРЕДОБАНК» необхідно завантажити з App Store, якщо відповідний пристрій працює на базі операційної системи Android мобільний застосунок Системи необхідно завантажити з Play Market).
15. Обмежте доступ до Робочого місця неуповноваженим особам.
16. Забезпечуйте доступність Удосконаленого ЕП для Системи/ Удосконаленого ЕП з кваліфікованим сертифікатом/Кваліфікованого ЕП на Робочому місці тільки в період роботи Користувача з Системою/ Системою онлайн-банкінгу «КРЕДОБАНК».
17. При виявленні незвичної поведінки Системи/Системи онлайн-банкінгу «КРЕДОБАНК» чи будь-яких змін в її інтерфейсі – негайно звертайтеся в Контакт-центр для з'ясування, чи не пов'язані такі зміни з оновленням програмного забезпечення Системи/ Системи онлайн-банкінгу «КРЕДОБАНК».
18. При виникненні підозри, що має місце НСК/НСД, негайно повідомляйте про це Банк шляхом звернення в Контакт-центр.
19. Використовуйте послугу СМС-повідомлень про рух коштів на Рахунку як оперативний засіб контролю за рухом коштів.

20. Не надавайте будь-кому конфіденційні дані, які використовуються для роботи в Системі/ Системі онлайн-банкінгу «КРЕДОБАНК», оскільки Банк за жодних обставин не здійснює розсилку електронних листів, СМС чи

інших повідомлень із вимогою уточнити чи надати конфіденційні дані Клієнта (Користувачів), подібні повідомлення є шахрайськими (фішинг).

21. Забезпечте розблокування екрану Мобільного телефону за допомогою паролю/FaceID/TouchID.
22. Використовуйте різні PIN-коди та паролі до Мобільного пристрою та додатків, зокрема до банківських мобільних застосунків онлайн-банкінгу;
23. Не встановлюйте додатків, отриманих з невідомих джерел та таких, робота яких вам не зрозуміла чи які вимагають велику кількість додаткових інсталяцій;
24. Під час встановлення додатків на Мобільний пристрій, перевіряйте, які права додаток вимагає (право віддаленого керування пристроєм тощо) та не встановлюйте додатки, які вимагають права, що можуть дозволити використання Мобільного пристрою іншими особами та/або отримувати конфіденційні дані, які використовуються для роботи в Системі/Системі онлайн-банкінгу «КРЕДОБАНК»;
25. Своєчасно встановлюйте доступні оновлення операційної системи і додатків на своєму Мобільному пристрої, що використовується для підключення Користувача до Системи/ Системи онлайн-банкінгу «КРЕДОБАНК».
26. Якщо виникли підозри, що телефон заражений вірусами, не вводьте чутливу інформацію (логіни, паролі, тощо) поки не перевірите ліцензійним антивірусним програмним забезпеченням та/або не звернетесь за допомогою до фахівців.
27. У випадку втрати Мобільного пристрою чи непрацездатності SIM-карти – зверніться до мобільного оператора та за потреби до Банку. Повідомте про це та обмежте доступ до Системи/Системи онлайн-банкінгу та особистого кабінету оператора зв'язку до моменту з'ясування обставин та відновлення роботи.
28. Дотримуйтесь інших заходів інформаційної безпеки, визначених Правилами, а також викладених на Інтернет-сторінці Банку.

Зверніть увагу!

Банк ніколи, за жодних обставин не здійснює розсилку електронних листів, SMS чи інших повідомлень із вимогою уточнити чи надати Ваші конфіденційні дані (в тому числі Особистого робочого ключа, Логіна, пароля, Одноразового пароля), подібні повідомлення є шахрайськими (фішинг).

БАНК:	КЛІЄНТ:
[вказане нижче для паперового документа]	*[вказане нижче для паперового документа]*
_____	_____
(П.І.Б. уповноваженої особи Банку, підпис)	(П.І.Б. керівника, підпис)
	_____
	(П.І.Б. гол. бухгалтера, підпис)
М.П.	М.П.
[вказане нижче для електронного документа]	*[вказане нижче для електронного документа]*
	_____
_____	_____*[для електронної заяви]*
(посада, прізвище, ініціали)	(посада,прізвище,ініціали)
	[для електронної заяви, що підписується із доступом через QR-код Клієнтом-ФОП кваліфікованим електронним підписом]
Підписано представником Банку згідно з кваліфікованим електронним підписом Банку.	*[для електронного Додатку, крім такого, що підписується із доступом через QR-код Клієнтом-ФОП кваліфікованим електронним підписом]*
	Підпис: ця Заява підписана ЕП Клієнта відповідно до Правил та / або законодавства України. *[для електронної заяви]*
	_____*[за потреби; для електронної заяви]*
	(посада, прізвище, ініціали)
Підпис: ця Заява підписана кваліфікованим електронним підписом Банку відповідно до законодавства України.*[для електронної заяви]*	Підпис: ця Заява підписана ЕП Клієнта відповідно до Правил та / або законодавства України. *[за потреби; для електронної заяви]*