ПАМЯТКА ПО БЕЗОПАСНОСТИ
ОБСЛУЖИВАНИЯ СИСТЕМЫ ДБО ДЛЯ ФИЗИЧЕСКИХ ЛИЦ

АО АКБ «Новикомбанк» придает большое значение обеспечению безопасности доступа к средствам Клиентов. Пожалуйста, внимательно прочитайте нижеизложенную информацию и следуйте нашим рекомендациям по работе с системой ДБО (далее - Система):

1. Вход в Систему осуществляется **ТОЛЬКО** через корпоративный сайт АО АКБ «НОВИКОМБАНК» (далее – Банк) https://novikom.ru/ и официальное мобильное приложение Банка.

2. Если вам пришли письма, в том числе от имени Банка, содержащие требования (а так же просьбы или предложения) зайти на сайт, адрес которого начинается не с адреса банка https://novikom.ru/, прислать секретный ключ или пароль доступа к Системе, **НИ В КОЕМ СЛУЧАЕ** не отвечайте. Вам нужно немедленно сообщить об этом в Банк в рабочее время по телефону **+7 (800) 250-70-07** Банк **НИКОГДА** не рассылает Клиентам подобные электронные письма, а также не рассылает по электронной почте программы для установки на компьютеры.

3. **НИКОГДА** не отлучайтесь от компьютера или мобильного устройства, пока работаете в Системе.

4. После завершения работы в Системе **СРАЗУ** нажимайте кнопку «Выход».

5. Пользоваться средствами генерации (получения) одноразовых паролей может **ТОЛЬКО** Клиент.

6. **НИ В КОЕМ СЛУЧАЕ** не передавайте средства генерации (получения) одноразовых паролей другим пользователям (в том числе ИТ-специалистам) даже для проверки работы Системы или настроек взаимодействия с Банком, и т. п. При необходимости такой проверки **ТОЛЬКО** Клиент должен использовать средства генерации (получения) одноразовых паролей, при этом убедившись, что пароли вводится именно в интерфейс клиентской части Системы.

7. **ОБЯЗАТЕЛЬНО** храните средства генерации (получения) одноразовых паролей, в надежном месте, исключающем их повреждение и несанкционированный доступ к ним посторонних лиц. Вся ответственность за сохранность средств генерации (получения) одноразовых паролей полностью лежит на вас, как единственном их владельце.

8. Вы должны обеспечить строго конфиденциальное использования паролей доступа и средств генерации (получения) одноразовых паролей. Работникам Банка для вашего обслуживания и поддержки Системы в работоспособном состоянии пароли **НЕ ТРЕБУЮТСЯ**.

9. **ОБЯЗАТЕЛЬНО** применяйте средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.

10. Как можно **БЫСТРЕЕ** производите смену паролей доступа или средств генерации (получения) одноразовых паролей, как в случае их рассекречивания, так и по требованию Банка.

11. В случае выявления явных или косвенных признаков рассекречивания паролей доступа или наличия вредоносных программ в компьютере или на мобильном устройстве, используемом для работы в Системе, вам нужно **НЕЗАМЕДЛИТЕЛЬНО уведомить об этом Банк** по телефону: **+7(800) 250-70-07**, либо лично явиться в Банк, чтобы заблокировать пароли доступа, с последующей их заменой. О нарушении секретности могут свидетельствовать следующие события:
    - утеря средств генерации (получения) одноразовых паролей, даже если они потом обнаружатся;
    - выход из строя средств генерации (получения) одноразовых паролей, когда невозможно достоверно определить причину их поломки (и допустима возможность того, что это произошло в результате действий злоумышленника);
    - обнаружение факта или угрозы использования (копирования) паролей доступа, средств генерации (получения) одноразовых паролей;
    - получение доступа к Системе неуполномоченных лиц (несанкционированная отправка электронных документов);
    - обнаружение ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности.

12. Устанавливайте приложение для мобильного Банка и его обновления только из магазина приложений App Store и Google Play.

13. Установите пароль доступа к вашему мобильному устройству.

14. Не храните на мобильном устройстве конфиденциальную информацию (PIN коды платежных карт, пароли доступа, кодовое слово).

15. Удаляйте конфиденциальную информацию в случае передачи мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек устройства.

16. В случае утери мобильного устройства с установленным Мобильным банком или обнаружения блокировки SIM-карты без Вашего ведома, незамедлительно заблокируйте доступ, позвонив в Банк.

17. Всегда проверяйте содержание PUSH –уведомлений и SMS-сообщений с кодами подтверждения – каждое сообщение (уведомление) содержит данные о типе подтверждаемой кодом операции, точной сумме и получателе. Никогда не вводите код подтверждения, не соответствующий операции.

18. Соблюдайте общие правила безопасного использования мобильного устройства:
    - используйте только лицензионное программное обеспечение;
    - установите антивирус и регулярно обновляйте его;
    - избегайте настроек типа root и jailbreak;
    - не проходите по сомнительным ссылкам.

Помимо указанных выше правил Банк рекомендует также:

- **ИСКЛЮЧИТЬ** доступ посторонним лицам к компьютерам и мобильным устройствам, используемых для работы в Системе;
- На компьютерах и мобильных устройствах, используемых для работы в Системе, **ЗАПРЕТИТЬ** посещение всех интернет-сайтов, кроме необходимых для входа в Систему, а также установку развлекательных и игровых программ;
- Использовать **ТОЛЬКО** лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО;
- При обслуживании компьютера и мобильных устройств ИТ-специалистами контролировать **ВСЕ** выполняемые ими действия;
- В качестве дополнительных мер по обеспечению безопасности **ВОСПОЛЬЗОВАТЬСЯ** предоставляемой Банком возможностью установки ежедневных лимитов.