Приложение № 4
к Договору на обслуживание
клиентов в системе ДБО «iBank»

Общие правила по обеспечению информационной безопасности
при работе с Системой ДБО «iBank».

1. Клиент обязан обеспечить хранение информации о своих учётных данных для работы в Системе «iBank» способом, делающим их недоступным третьим лицам, а также немедленно уведомлять Банк о их компрометации.
2. Клиент может самостоятельно изменять пароль доступа к ЭП путем выполнения предусмотренной в Системе «iBank» процедуры смены пароля.
3. Клиент не должен сообщать свои пароли работникам Банка по телефону, электронной почте или иным способом. Использование пароля допускается только при работе Клиента непосредственно с Системой «iBank», без участия работников Банка.
4. Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения невозможности доступа посторонних лиц к информации о его учётных данных, находящихся в распоряжении Банка.
5. Клиент обязуется использовать для хранения Ключа ЭП электронный идентификатор Рутокен ЭЦП 2.0, выданный Банком.
6. Ключ электронной подписи должен использоваться только в целях подписи ЭД, подготовленных с помощью Системы «iBank».
7. Банк вправе ограничить число одновременно действующих Сертификатов ключей проверки ЭП.
8. Срок действия Сертификата ключа проверки ЭП устанавливается равным 1000 (тысяче) дней с момента регистрации Сертификата Банком.
9. Банк вправе, в случае возникновения любых сомнений в подлинности направленных Клиентом по Системе «iBank» ЭД, подозрений, возникновения событий, указывающих на компрометацию Ключа ЭП, в одностороннем порядке досрочно прекратить действие Сертификата ключа проверки ЭП с уведомлением об этом Клиента не позднее рабочего дня, следующего за датой принятия такого решения.
10. Клиентом должны быть назначены должностные лица, ответственные за осуществление мероприятий по обеспечению функционирования и безопасности ЭИ Рутокен ЭЦП. Клиент должен создать условия, обеспечивающие сохранность конфиденциальной информации, обрабатываемой с помощью ЭИ Рутокен ЭЦП.
11. Клиент самостоятельно должен обеспечивать контроль используемых для работы с ЭИ Рутокен ЭЦП операционных систем на наличие обновлений по безопасности и производить их своевременную установку.
12. Уполномоченные лица Клиента должны обеспечить конфиденциальность своих электронных подписей и не допускать использование принадлежащих им ключей электронных подписей без их согласия.
13. Клиентом должны быть регламентированы учет и хранение ЭИ Рутокен ЭЦП, непосредственная работа с ними, а также персональная ответственность за их сохранность.
14. Хранение ЭИ Рутокен ЭЦП допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение, несанкционированное использование.
15. После получения ЭИ Рутокен ЭЦП в Банке, Уполномоченные лица Клиента должны сменить код доступа (ПИН-код) к ЭИ Рутокен ЭЦП на известный только им.
16. Клиент должен обеспечить ознакомление с данными требованиями всех уполномоченных и ответственных лиц, допущенных к работе в Системе «iBank».
17. По возможности, не использовать для отправки платежных документов сеть Интернет с общественным доступом (Интернет-кафе, бесплатный Wi-Fi и пр.).
18. Регулярно контролировать состояние своих счетов и незамедлительно информировать ответственных сотрудников Банка обо всех подозрительных или несанкционированных операциях;
19. Выполнять незамедлительную блокировку и смену ключей ЭП в случаях их компрометации, по истечении срока действия ключей с периодичностью, установленной Банком.
20. Выполнять блокировку ключей ЭП во всех случаях увольнения или смены лиц, допущенных к этим ключам.
21. Настоятельно рекомендуется заменять ключи ЭП во всех случаях увольнения или смены руководителей юридического лица, которые подписывали распоряжения (доверенность) о предоставлении полномочий по подписи электронных документов ЭП.
22. Использовать на ПК, на которых осуществляется подготовка и отправка документов в Банк, программное обеспечение по защите от вредоносного кода (антивирусы) с актуальными вирусными базами, а также регулярно обновлять программное обеспечение в целях устранения выявленных в нем уязвимостей.
23. Исключить на ПК, на которых осуществляется подготовка и отправка документов в Банк, использование систем удаленного управления ПК.
24. Исключить посещение сомнительных сайтов, чтение почты и открытия почтовых вложений от недостоверных источников, установку и обновление любого программного обеспечения (ПО) не с сайтов производителей.
25. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.) ни при каких обстоятельствах не сообщать данную информацию.
26. При наличии проблемы с подключением к Системе ДБО «iBank» следует немедленно обратиться в службу поддержки Системе ДБО «iBank» Банка.
27. Любое информационное взаимодействие с Банком осуществлять только с использованием средств связи, реквизиты которых заранее оговорены в соответствующих приложения к Правилам.
28. При пользовании услугой **«Мобильный банк»** Клиент обязан соблюдать следующие требования безопасности:

- Хранить в секрете и не передавать третьим лицам пароли доступа к мобильному устройству, мобильному приложению «Банк Ермак – для бизнеса» и ключам ЭП;
- Не оставлять мобильное устройство, с установленным приложением **«Банк Ермак – для бизнеса»** или используемое для получения SMS-кода, без присмотра в местах, доступных для третьих лиц, и никому их не передавать;
- Устанавливать мобильное приложение «Банк Ермак – для бизнеса» только из авторизованных магазинов App Store и Play Market и только на принадлежащие Клиенту мобильные устройства;
- Использовать антивирусное программное обеспечение, в случае, если оно доступно для используемого Клиентом мобильного устройства;
- Не использовать приложение «Банк Ермак - для бизнеса» на устройствах, на которых повышены привилегии пользователя (получены root-права на Android устройствах и проведен jailbreak на iOs устройствах).

Для получения дополнительной информации обращайтесь в банковскую службу поддержки Системы ДБО «iBank» по телефону (3466) 49-50-53.