ПРИЛОЖЕНИЕ 1

К Условиям Договора дистанционного банковского обслуживания физических лиц в АО «ТРОЙКА-Д БАНК»с использованием системы «Тройка – Д Онлайн»

1. Ограничения при использовании системы «Тройка – Д Онлайн»

1.1. Для доступа к системе «Тройка – Д Онлайн» необходим персональный компьютер, ноутбук, планшет, устройство мобильной связи или иное устройство, предназначенное для выхода в интернет (далее – Компьютерное устройство), подключенное к сети Интернет. Требования, предъявляемые к оборудованию и программному обеспечению, необходимому для доступа к системе «Тройка – Д Онлайн» посредством доступа с Компьютерного устройства, содержатся на официальном сайте Банка www.troikabank.com.

1.2. В случае проведения технических работ на стороне Банка, может быть введено временное ограничение на предоставление информации по счетам Клиента в Банке. О наличии таких ограничений Банк уведомляет Клиента путем размещения сообщения в системе «Тройка – Д Онлайн»

2. Случаи повышенного риска, связанные с использованием системы «Тройка – Д Онлайн»

2.1. Клиент соглашается на получение услуги с использованием системы «Тройка – Д Онлайн», осознавая, что сеть Интернет не всегда является безопасным каналом связи и передачи информации, и осознает риски, связанные с возможным нарушением конфиденциальности, и иные риски, возникающие вследствие использования такого канала доступа, в частности риск осуществления переводов денежных средств Клиента лицами, не обладающими правом распоряжения этими денежными средствами.

2.2. Банк информирует Клиента о следующих случаях повышенного риска, связанных с использованием системы «Тройка – Д Онлайн» посредством доступа с Компьютерного устройства:

2.2.1. Использование системы «Тройка – Д Онлайн» с помощью Компьютерного устройства, размещенной в общественном месте. В случае необходимости такого использования Клиент может максимально обезопасить себя, выполнив условия обеспечения безопасности соединения в сети Интернет (п.3.2 настоящего Приложения);

2.2.2. Кража или потеря мобильного телефона, на номер которого приходят СМС-сообщения с Разовыми Секретными Паролями для подтверждения операций по счету посредством системы «Тройка – Д Онлайн» В случае подозрения на кражу или потерю мобильного телефона Клиент обязан незамедлительно обратиться в Офис Банка или по телефону в Единый информационный центр Банка для временной блокировки доступа к системе «Тройка – Д Онлайн» (до восстановления SIM-карты) или изменения номера мобильного телефона;

2.2.3. Невыполнение условий обеспечения безопасности автоматизированного рабочего места (далее - АРМ), с которого осуществляется доступ в систему «Тройка – Д Онлайн» (п.3.3 настоящего Приложения);

2.2.4. Использование Пароля, не соответствующего минимальным требованиям к безопасности (п.3.4 настоящего Приложения).

2.2.5. Получение доступа к системе «Тройка – Д Онлайн» посредством браузера с устройства, содержащего вредоносный или модифицированный код, а также с устройств, на которых произведена модификация системы с целью получения доступа к файловой системе или иных прав, не предусмотренных разработчиками операционной системы.

3. Меры обеспечения безопасности при пользовании системой «Тройка – Д Онлайн» посредством доступа с компьютерного устройства.

3.1. Клиент обязан исключить доступ третьих лиц к Паролю (в том числе Временному паролю, Разовому Секретному Паролю) и Логину:

3.1.1. Хранить Пароль и Логин раздельно в недоступных для третьих лиц местах.

3.1.2. Незамедлительно обратиться в Банк для смены Пароля в случае появления подозрений в том, что Пароль мог оказаться известен третьим лицам.

3.2. Клиент должен обеспечить безопасность соединения в сети Интернет (при доступе с Компьютерного устройства, если не указано иное):

3.2.1. Собственноручно переходить по ссылке, размещенной на официальном сайте Банка www.troikabank.com.

3.2.2. Не переходить на сайт системы «Тройка – Д Онлайн» по ссылкам, размещенным в электронных письмах или размещенным на сайтах в сети Интернет (кроме официального сайта Банка www.troikabank.com).

3.3. Клиент должен обеспечить безопасность АРМ, с которого осуществляется доступ в систему «Тройка – Д Онлайн»:

3.3.1. Допускать к работе на АРМ только доверенных лиц, обеспечить физическую безопасность устройства, на котором установлен АРМ.

3.3.2. Использовать на АРМ только лицензионное программное обеспечение.

3.3.3. Использовать АРМ, на котором установлена только одна операционная система.

3.3.4. Работать в операционной системе АРМ под локальной учетной записью с ограниченными правами доступа.

3.3.5. Установить на АРМ специальные программные и аппаратные средства защиты (антивирусное программное обеспечение, средства обнаружения вредоносных программ, персональный межсетевой экран), которые должны регулярно обновляться.

3.3.6. Производить регулярное обновление программного обеспечения, установленного на АРМ.

3.3.7. Запускать на АРМ программы, полученные только из доверенных источников (особую опасность могут представлять программы, полученные по электронной почте или из сети Интернет); не рекомендуется открывать и использовать без проведения соответствующих проверок файлы, полученные из общедоступных сетей передачи данных, для исключения программных закладок и вирусов.

3.3.8. Установить парольную защиту на вход в АРМ и мобильный телефон.

3.3.9. Регулярно проводить смену Паролей.

3.4. При установке Пароля рекомендуется придерживаться следующих правил:

3.4.1. Длина Пароля – не менее 8 символов.

3.4.2. Пароль не должен совпадать ни с одним из последних трех Паролей, ранее использованных Клиентом.

3.4.3. Пароль не должен совпадать с Логином.

3.4.4. В Пароле должны присутствовать символы из разных регистров (большие и маленькие буквы) и цифры. Для предотвращения возможных осложнений, связанных с различной кодировкой, рекомендуется использовать «латиницу».

3.4.5. Пароль не должен целиком состоять из комбинации символов, несущей смысловую нагрузку. Не рекомендуется использовать имена, названия, общепринятые аббревиатуры, адреса или другие общеизвестные слова и их сочетания, в том числе русское слово, набранное в латинской транскрипции (например: ФАМИЛИЯ - AFVBKBZ);

3.4.6. Последовательность символов Пароля не должна иметь очевидных закономерностей (например: Пароли 11111111, 12121212, 12345678, QWERTY имеют очевидные зависимости между своими символами).

3.5. Клиент обязан внимательно знакомиться с информационными сообщениями Банка по безопасности, размещенными на сайте Банка, направленными по электронной почте или посредством СМС-сообщения. Если имеются сомнения в достоверности адреса отправителя сообщения, необходимо обратиться в Единый информационный центр Банка, по телефону, указанному на сайте Банка.