УТВЕРЖДЕНО
Приказом Генерального директора
АО «ДК РЕГИОН»
Приказ № ДК- 43Д от «08» сентября 2026 г.

Дата вступления в силу 23.09.2026 г.

СОГЛАШЕНИЕ № _____/ EDO
об электронном документообороте

г. Москва «_ _» _____ 20___

_____ «_____» именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____ с одной стороны,

Акционерное общество «Депозитарная компания «РЕГИОН», действующее на основании лицензии №22–000–0-00088 от 13.05.2009 на осуществление деятельности специализированного депозитария инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, а также

лицензии профессионального участника рынка ценных бумаг на осуществление депозитарной деятельности № 045-09028-000100 от 04.04.2006,

именуемое в дальнейшем «Компания», в лице _____, действующего на основании _____, с другой стороны,

принимая во внимание, что Сторонами в отдельности были заключены Договоры о присоединении к системе электронного документооборота (далее «Договор о присоединении к СЭД») с Обществом с ограниченной ответственностью «Центр информационных технологий «РЕГИОН» (далее «Организатор СЭД»), а именно:

– между Компанией и Организатором СЭД - Договор о присоединении к СЭД от 26.11.2012 № СЭД261112-1;

– между Клиентом и Организатором СЭД - Договор о присоединении к СЭД от ___.___._____ №_____,

а также руководствуясь положениями Правил электронного документооборота в системе электронного документооборота Общества с ограниченной ответственностью «Центр информационных технологий «РЕГИОН», разработанных и утвержденных Организатором СЭД,

совместно именуемые «Стороны», заключили настоящее соглашение (далее – Соглашение) о нижеследующем.

В соответствии с Соглашением Стороны договорились осуществлять электронный документооборот (далее – ЭДО) между Сторонами в электронной форме с электронной подписью с использованием следующих систем (далее – Системы ЭДО):

а) системы ЭДО Общества с ограниченной ответственностью «Центр информационных технологий «РЕГИОН» (далее – СЭД). ЭДО организовано и обеспечивается Организатором СЭД в соответствии с Правилами электронного документооборота в системе электронного документооборота Общества с ограниченной ответственностью «Центр информационных технологий «РЕГИОН» (далее – Правила ЭДО), являющимися неотъемлемой частью Договоров о присоединении к СЭД, в рамках взаимодействия между Компанией и Клиентом;

б) системы ЭДО «Личный кабинет клиента» АО «ДК РЕГИОН» при условии подключения к ней Клиента (далее – ЛКК).

Клиент самостоятельно производит все действия, предусмотренные Регламентом Системы ЭДО ЛКК, необходимые для подключения Клиента к ЛКК. Регламент Системы ЭДО ЛКК

опубликован в сети Интернет по адресу: http://region-dk.ru/raskrytie-informatsii/depozitarnaya-kompaniya-region/elektronnyy-dokumentooborot/;

в) системы ЭДО «Контур.Диадок» оператора АО «ПФ «СКБ КОНТУР» (ИНН 6663003127), если Клиент использует эту систему или систему ЭДО другого оператора, которая позволяет обмениваться электронными документами с пользователями системы ЭДО «Контур.Диадок» (роуминг), - для обмена в электронном виде счетами по оплате услуг Компании, актами оказанных услуг, актами сверки, УПД и счетами-фактурами (при необходимости), дополнительными соглашениями к Соглашению (далее – Диадок).

В целях Соглашения используются следующие термины и определения**.**

Договоры – следующие договоры (соглашения) в действующей редакции, заключенные (или которые могут быть заключены в будущем) Сторонами настоящего Соглашения:

- Депозитарный договор;
- Договор на оказание услуг специализированного депозитария ипотечного покрытия;
- Договор на оказание услуг специализированного депозитария (с управляющей компанией паевого инвестиционного фонда);
- Договор на оказание услуг по ведению реестра владельцев инвестиционных паев;
- иные договоры, в которых Сторонами прямо предусмотрено применение настоящего Соглашения для взаимодействия Сторон.

Шаблон – совокупность установленных Компанией требований к Форме документа и Формату файла. В отношении файлов, обмен которыми Стороны будут осуществлять в Формате *.xml, понятие Шаблон включает в себя XML–схему, предоставляемую Компанией Клиенту.

Требования к Шаблонам определены в Приложении № 1 к Соглашению.

Форма документа - модель построения документа, устанавливающая область применения, размеры полей, требования к построению конструкционной сетки и основные реквизиты документа. Форма документа устанавливается Договорами.

Формат файла - спецификация структуры данных, записанных в виде последовательности байтов в компьютерном файле. Формат файла определяет порядок (алгоритм) преобразования структурированных данных в последовательность байтов, образующих файл, и обратно.

Термины и определения, для которых не определены значения в настоящем Соглашении, определяются в значениях, закрепленных Правилами ЭДО и Договором о присоединении к СЭД.

1. Общие положения

Стороны согласились, что:

1.1. Все термины и определения в целях Соглашения применяются в значениях, определенных Соглашением, Правилами ЭДО и Договором о присоединении к СЭД, а также действующим законодательством РФ и нормативными актами Банка России.

1.2. Все правоотношения в рамках Договоров, вытекающие из предоставления/получения документов в бумажном виде, распространяются и на переданные посредством Систем ЭДО электронные документы, подписанные электронной подписью (далее – ЭП).

1.3. При взаимодействии посредством СЭД Стороны используют усиленную (квалифицированную или неквалифицированную) электронную подпись, проверка подлинности которой осуществляется в порядке, установленном Правилами ЭДО.

При взаимодействии посредством ЛКК или Диадок Стороны используют усиленную квалифицированную электронную подпись.

1.4. Компания в срок, не превышающий 3 (Трех) рабочих дней с момента заключения настоящего Соглашения, обязуется предоставить Клиенту XML-схемы, предназначенные для формирования XML-документов, обмен которыми предусмотрен в Приложении № 1. Документы, для которых Приложением № 1 к Соглашению предусмотрены Шаблоны, Компания обязуется принимать, а Клиент направлять с использованием СЭД или ЛКК в соответствии с установленными Шаблонами. Компания вправе изменять ранее предоставленные Клиенту XML-схемы в период действия Соглашения, уведомив Клиента о таких изменениях не позднее, чем за 30 календарных дней до момента вступления изменений в силу.

1.5. Документы, для которых Приложением № 1 не предусмотрены Шаблоны, Компания обязуется принимать, а Клиент направлять в виде подписанных ЭП файлов произвольного Формата, который позволяет после успешной проверки ЭП однозначно воспринять содержание документов с применением стандартных средств Microsoft Office или Adobe, без применения дополнительных технических средств.

1.6. В случае получения от Клиента документов, не соответствующих требованиям к Форме документов, Шаблонам или Форматам файлов, Компания уведомляет Клиента о выявленных несоответствиях и оставляет за собой право не принимать указанные документы к исполнению. Компания не несет ответственность за возникшие в таких случаях убытки Клиента.

1.7. Стороны незамедлительно (в тот же рабочий день) обязаны извещать Удостоверяющий центр (Аккредитованный удостоверяющий центр), а также другую Сторону о случаях компрометации ключа электронной подписи (далее – ключи ЭП), а также об иных случаях нарушения конфиденциальности ключей ЭП посредством направления сообщения по электронной почте по адресу, указанному в разделе 6 Соглашения. С момента получения сообщения от Стороны Соглашения о компрометации ключа ЭП другая Сторона обязуется не исполнять поручения, требования и запросы, подписанные с использованием компрометированного ключа ЭП. С Даты компрометации ключа ЭП электронные документы, подписанные с помощью ключа ЭП, соответствующего Сертификату, помещенному в Список отозванных сертификатов, не имеют юридической силы.

2. Порядок и условия взаимодействия Сторон

2.1. Обслуживание Клиента производится в сроки, в порядке и на условиях, определенных в Договорах и настоящем Соглашении.

2.2. Предоставление Компанией услуг, предусмотренных Договорами, осуществляется на основании электронных документов, представленных Клиентом Компании.

2.3. Отчеты о проведенных операциях, а также иные документы, указанные в Приложении № 1 в отношении каждого из Договоров, предоставляются Клиенту в виде электронных документов, подписанных ЭП, если Стороны не договорились об ином порядке их предоставления.

2.4. Моментом получения электронного документа, направленного с помощью СЭД, является момент попадания электронного документа с ЭП в папку «На регистрацию» получателя.

Моментом получения электронного документа, направленного с помощью ЛКК, является дата размещения отправителем подписанных УКЭП документов и информации в ЛКК в соответствии с Регламентом Электронного документооборота Системы «Личный кабинет клиента» АО «ДК РЕГИОН».

Моментом получения электронного документа, направленного с помощью ЛКК, является дата размещения отправителем подписанных УКЭП документов и информации в ЛКК в соответствии с Регламентом Электронного документооборота Системы «Личный кабинет клиента» АО «ДК РЕГИОН».

2.5. Сторона-получатель не несет ответственности за несвоевременную обработку электронного документа в случае временного отсутствия доступа Стороны-получателя к СЭД по причине, не зависящей от Сторон настоящего Соглашения. При этом Стороны обязуются обеспечивать документооборот иными доступными для обеих Сторон способами вплоть до восстановления доступа к СЭД.

2.6. Электронный документ имеет силу и влечет предусмотренные для данного документа последствия с момента его получения при одновременном соблюдении следующих условий:

- электронный документ оформлен согласно п. п. 1.3. и 1.4. Соглашения;

- получателем электронного документа получен положительный результат проверки ЭП отправителя.

3. Ответственность Сторон

3.1. При разрешении разногласий, связанных с использованием Сторонами ЭДО и/или возникающих при использовании ЭП, Стороны руководствуются положениями Договора о

присоединении к СЭД, Правилами ЭДО, Регламентом Системы ЭДО ЛКК, правилами работы системы ЭДО «Контур.Диадок», а также законодательством РФ.

3.2. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по настоящему Соглашению.

3.3. Компания несет ответственность за:

3.3.1. убытки Клиента, возникшие вследствие своевольного изменения Компанией документа, подписанного ЭП;

3.3.2. действия сотрудников Компании, связанные с неправомерным и/или неквалифицированным использованием ключей ЭП, повлекших убытки Клиента.

3.4. Компания не несет ответственность за:

3.4.1. убытки Клиента, возникшие вследствие компрометации либо неправомочного и/или неквалифицированного использования Клиентом ключей ЭП, о чем Компания не была уведомлена в сроки и порядке, предусмотренными п. 1.7. Соглашения или была уведомлена с нарушением этих сроков;

3.4.2. действия сотрудников Клиента и передачу ими электронных документов в адрес Компании, повлекшие убытки Клиента в рамках осуществления Договоров;

3.4.3. убытки Клиента, возникшие ввиду неисполнения Компанией требований, распоряжений, запросов Клиента, не соответствующих требованиям Компании к Шаблонам таких документов.

3.5. Клиент несет ответственность за:

3.5.1. достоверность и своевременность предоставления информации, которая предоставляется в рамках взаимоотношений Сторон;

3.5.2. действия сотрудников Клиента, связанные с неправомерным и/или неквалифицированным использованием ключей ЭП, повлекших убытки Клиента и/или Компании;

3.5.3. несвоевременность уведомления Компании о случаях компрометации ключей ЭП.

3.6. Клиент не несет ответственность за:

3.6.1. убытки Компании, возникшие вследствие компрометации либо неправомочного и/или неквалифицированного использования Компанией ключей ЭП, о чем Клиент не был уведомлен в сроки и порядке, предусмотренными п. 1.7. Соглашения или был уведомлен с нарушением этих сроков;

3.6.2. убытки, возникшие вследствие изменения Компанией электронных документов, поступивших Компании;

3.6.3. действия сотрудников Компании, связанные с неправомерным и/или неквалифицированным использованием ключей ЭП, повлекших убытки Клиента и/или Компании.

3.7. Ни одна из Сторон не несет ответственность за полное или частичное неисполнение обязательств по настоящему Соглашению, если неисполнение обязательств вызвано наступлением обстоятельств непреодолимой силы (форс-мажор), таких как стихийные бедствия, забастовки, акты государственных органов, выход из строя средств связи и другие обстоятельства, находящиеся вне разумного контроля Сторон и препятствующие передаче и приему какой-либо из Сторон каких-либо согласованных Сторонами электронных сообщений.

3.8. Сторона, в отношении которой наступили указанные в п. 3.7. настоящего Соглашения обстоятельства, обязана в течение одного дня с момента наступления таких обстоятельств известить об этом другую Сторону. При этом вторая Сторона вправе потребовать представления ей доказательств, которыми могут служить справки и свидетельства, выдаваемые соответствующими органами власти и управления, за исключением случаев, когда такие обстоятельства являются общеизвестными. В случае нарушения срока уведомления, указанного в настоящем пункте, Сторона лишается права ссылаться на вышеуказанные обстоятельства как освобождающие от ответственности за неисполнение своих обязательств.

3.9. В случае прекращения действия обстоятельств непреодолимой силы Стороны обязаны сообщать об этом друг другу в течение одного рабочего дня с момента их прекращения.

3.10. Клиент при подписании настоящего Договора уведомлен о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющих право совершать транзакции от лица клиента, изложенных в Приложении № 2 к Соглашению.

4. Срок действия Соглашения и порядок его расторжения

4.1. Настоящее Соглашение вступает в силу с момента его подписания обеими Сторонами.

4.2. Срок действия настоящего Соглашения не может превышать срок действия Договора о присоединении к СЭД. В отношении каждого из Договоров настоящее Соглашение действует до момента прекращения обязательств по таким Договорам.

4.3. Настоящее Соглашение может быть досрочно расторгнуто по желанию любой из Сторон. Сторона, желающая расторгнуть Соглашение, письменно уведомляет об этом другую Сторону. С момента получения уведомления Компания не принимает электронные документы Клиента, влекущие обязанность Компании осуществить какие-либо юридические действия.

4.4. В случае если настоящим Соглашением предусмотрены иные правила взаимоотношений Сторон, чем те, которые содержатся в Договоре о присоединении к СЭД и Правилах ЭДО, применяются правила настоящего Соглашения.

5. Прочие положения

5.1. Сторона, получившая доступ к персональным данным, которые были переданы другой Стороной в рамках исполнения Соглашения, обязуются не раскрывать их третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством РФ.

5.2. Настоящее Соглашение составлено в 2-х экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон. Каждый экземпляр подписывается уполномоченными лицами и скрепляется печатями.

5.3. Все приложения и дополнения к настоящему Соглашению являются его неотъемлемой частью и должны быть подписаны уполномоченными представителями обеих Сторон.

6. Реквизиты и подписи Сторон

Компания:	**Клиент:**
Акционерное общество «Депозитарная компания «РЕГИОН»	_____
Адрес в пределах места нахождения: 119049, г. Москва, вн. тер. г. муниципальный округ Якиманка, ул. Крымский вал, д. 3, стр. 2, антресоль 3, помещ. I ком.32-57	Адрес в пределах места нахождения: _____ _____
ИНН 7708213619, КПП 997950001	ИНН _____, КПП _____
р/с 40701810600760013745	р/с _____
в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»	в _____
к/с 30101810745250000659	к/с _____
БИК 044525659	БИК _____
Тел. +7 (495) 777-29-64	Тел. +7 (____) _____
e-mail: depo@region.ru	e-mail: _____
_____ /_____/	_____ /_____/
М.П.	М.П.

Приложение № 1

к Соглашению об электронном документообороте
№ _____/EDO
от «___» _____ 20___

Требования к Шаблонам электронных документов

I. Шаблоны документов, обмен которыми осуществляется в рамках Депозитарного договора:

Формат файла: *.xls
Формы документов: установлены Регламентом депозитарного обслуживания Акционерного общества «Депозитарная компания «РЕГИОН».

II. Шаблоны документов, обмен которыми осуществляется в рамках Договора на оказание услуг специализированного депозитария (с управляющей компанией паевого инвестиционного фонда):

Формат файла: *.xls
Формы документов установлены:

- Регламентом специализированного депозитария инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов АО «ДК РЕГИОН»;
- Правилами ведения реестра владельцев инвестиционных паев паевых инвестиционных фондов специализированного депозитария АО «ДК РЕГИОН»;
- Регламентом депозитарного обслуживания Акционерного общества «Депозитарная компания «РЕГИОН».

III. Шаблоны документов, обмен которыми осуществляется в рамках Договора на оказание услуг по ведению реестра владельцев инвестиционных паев:

Формат файла: *.xls
Формы документов: установлены Правилами ведения реестра владельцев инвестиционных паев паевых инвестиционных фондов специализированного депозитария АО «ДК РЕГИОН».

IV. Шаблоны документов, обмен которыми осуществляется в рамках Договора на оказание услуг специализированного депозитария ипотечного покрытия:

Наименование документа: **Распоряжение**
Формат файла: *.xml в соответствии с представленной Компанией XML-схемой
Форма документа: установлена Регламентом специализированного депозитария ипотечного покрытия Акционерного общества «Депозитарная компания «РЕГИОН».

Наименование документа: **Акт приема-передачи**
Формат файла: *.xls, *.xlsx, *.doc, *.pdf
Форма документа: установлена Регламентом специализированного депозитария ипотечного покрытия Акционерного общества «Депозитарная компания «РЕГИОН» (Форма 8 АРВТИЗ, Форма 10 АРВТИЗ, Форма 12 АРВНИ, Форма 18 АРИТОИО, Форма 20 АРИзСДС).

Наименование документа: **Уведомление и приложения к уведомлению/выписке**
Формат файла: *.xls, *.xlsx, *.doc, *.pdf
Форма документа: установлена Регламентом специализированного депозитария ипотечного покрытия Акционерного общества «Депозитарная компания «РЕГИОН» (Форма 1 УФНВН,

Форма 2 УФНВН, Форма 3 УФНВН, Форма 4 УО, Форма 5 УВИ, Форма 6 УИИ, Форма 7 УИзС, Формы 8 - 13).

Наименование документа: **Выписка из реестра**
Формат файла: *.xls, *.xlsx, *.doc, *.pdf
Форма документа: установлена Регламентом специализированного депозитария ипотечного покрытия Акционерного общества «Депозитарная компания «РЕГИОН» (Форма 14 ВР).

Наименование документа: **Реестр ипотечного покрытия**
Формат файла: *.xls, *.xlsx, *.doc, *.pdf
Форма документа: установлена Регламентом специализированного депозитария ипотечного покрытия Акционерного общества «Депозитарная компания «РЕГИОН» (Форма 18 РИП).

Наименование документа: **Справка о размере ипотечного покрытия**
Формат файла: *.xls, *.xlsx, *.doc, *.pdf
Форма документа: установлена Регламентом специализированного депозитария ипотечного покрытия Акционерного общества «Депозитарная компания «РЕГИОН» (Форма 15 СРИПО и Форма 16 СРИПСУ).

Подписи Сторон

Компания:	**Клиент:**
Акционерное общество «Депозитарная компания «РЕГИОН»	**_____**
_____ /_____/	_____ /_____/
М.П.	М.П.

Приложение № 2

к Соглашению об электронном документообороте
№ _____/EDO
от «___» _____ 20___

Уведомление клиентов о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц, не имеющих право совершать транзакции от лица клиента.
Рекомендации клиентам по защите от противоправного доступа и о рисках вредоносных программ

I. Уведомление о рисках информационной безопасности, связанных с несанкционированным доступом, вредоносными кодами и иными противоправными действиями лиц.

В соответствии с требованиями Положения об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций (утв. Банком России 20.04.2021 № 757-П) **Акционерное общество «Депозитарная компания «РЕГИОН»** (далее – «Общество») настоящим **уведомляет** клиентов Общества о возможных рисках финансовых потерь из-за:

- несанкционированного доступа к Вашей информации лицами, не обладающими правом осуществления финансовых операций;
- потери (хищения) носителей ключей электронной подписи, с использованием которых осуществляются финансовые операции;
- воздействия вредоносного кода на устройства, с которых совершаются финансовые операции;
- совершения в отношении Вас иных противоправных действий.

При осуществлении финансовых операций следует принимать во внимание риск получения третьими лицами несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, такие риски могут быть обусловлены включая, но не ограничиваясь следующими примерами:

a. Кража пароля и идентификатора доступа или иных конфиденциальных данных, например, закрытого ключа посредством технических средств и/или вредоносного кода и использование злоумышленниками указанных данных с других устройств для несанкционированного доступа.

b. Установка на устройство вредоносного кода, который позволит злоумышленникам осуществить операции от Вашего имени.

c. Использования злоумышленником утерянного или украденного телефона для получения СМС кодов, которые могут применяться Обществом в качестве дополнительной защиты для несанкционированных финансовых операций, что позволит им обойти защиту.

d. Кража или несанкционированный доступ к устройству, с которого Вы пользуетесь услугами/сервисами Общества для получения данных и/или несанкционированного доступа к сервисам с этого устройства.

e. Получение пароля и идентификатора доступа и/или кода из СМС и/или кодового слова и прочих конфиденциальных данных, в т.ч. паспортных данных, номеров счетов и т.д. путем обмана и/или злоупотребления доверием, когда злоумышленник представляется сотрудником Общества или техническим специалистом или использует иную легенду и просит Вас сообщить ему эти секретные данные; или направляет поддельные почтовые сообщения или письмо по обычной почте с просьбой предоставить информацию или совершить действие, которое может привес к компрометации устройства.

f. Перехват почтовых сообщений и получение несанкционированного доступа к выпискам, отчетам и прочей финансовой информации, если Ваша почта используется для информационного обмена с Обществом. В случае получения доступа к вашей почте, - отправка сообщений от Вашего имени в Общество.

Все риски, связанные с утратой и компрометацией учётных данных (логин, пароль) для доступа к информационным системам Общества несет Владелец учётных данных.

Общество не несет ответственность в случаях финансовых потерь, понесенных клиентами в связи с пренебрежением правилами информационной безопасности.

II. Меры по предотвращению несанкционированного доступа к защищаемой информации.

1. Обеспечьте защиту устройства, с которого вы пользуетесь услугами Общества. К таким мерам включая, но не ограничиваясь могут быть отнесены:
   - Использование только лицензированного программного обеспечения, полученного из доверенных источников.
   - Запрет на установку программ из непроверенных источников.

- Наличие средства защиты, таких как: антивирус (с регулярно и своевременно обновляемыми базами), персональный межсетевой экран, защита накопителя.
- Настройка прав доступа к устройству с целью предотвращения несанкционированного доступа.
- Хранение, использование устройства с целью избежать рисков кражи и/или утери.
- Своевременные обновления операционной системы.
- Активация парольной или иной защиты для доступа к устройству.
- В случае обнаружения злонамеренного программного обеспечения на компьютере после его удаления незамедлительно смените логин и пароль.
- Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины.

2. Обеспечьте конфиденциальность:
   - Храните в тайне аутентификационные/идентификационные данные и ключевую информацию, полученные от Общества: пароли, СМС коды, кодовые слова, закрытые ключи, сертификаты, а в случае компрометации немедленно примите меры для смены и/или блокировки;
   - Соблюдайте принцип разумного раскрытия информации о номерах счетов, о ваших паспортных данных, о номерах кредитных и дебетовых карт, о CVC кодах, в случае если у вас запрашивают указанную информацию, в привязке к сервисам Общества по возможности оцените ситуацию и уточните полномочия и процедуру через независимый канал, например, через телефон контакт центра Общества.
3. Проявляйте осторожность и предусмотрительность:
   - Будьте осторожны при получении писем со ссылками и вложениями, они могут привести к заражению вашего устройства вредоносным кодом. Вредоносный код, попав к Вам через почту или интернет-ссылку на сайт, может получить доступ к любым данным и информационным системам на вашем устройстве.
   - Внимательно проверяйте адресата, от которого пришло письмо. Входящее письмо может быть от злоумышленника, который маскируется под Общество или иных доверенных лиц.
   - Будьте осторожны при просмотре/работе с интернет-сайтами, так как вредоносный код может быть загружен с сайта.
   - Будьте осторожны с файлами в архиве с паролем, так как в таком файле может быть вредоносный код.
   - Не заходите в системы удаленного доступа с недоверенных устройств, которые вы не контролируете. На таких устройствах может быть вредоносный код, собирающий пароли и идентификаторы доступа или способный подменить операцию.
   - Анализируйте информацию в прессе и на сайте Общества о последних критичных уязвимостях и о вредоносном коде.
   - При наличии в рамках вашего продукта сервиса контакт-центра, осуществляйте звонок только по номеру телефона, указанному в договоре. Важно учесть, что от лица Общества не могут поступать звонки или сообщения, в которых от Вас требуют передать СМС-код, пароль, номер карты, кодовое слово и т.д.
   - Имейте в виду, что если Вы передаете ваш телефон и/или устройство другим пользователям, они могу установить на него вредоносный код, а в случае кражи или утери злоумышленники могут воспользоваться им для доступа к системам Общества, которыми пользовались Вы.
   - При утере, краже телефона, используемого для получения СМС кодов или доступа к системам Общества, необходимо:
     a. незамедлительно проинформировать Общество через контактный центр;
     b. целесообразно по возможности оперативно с учетом прочих рисков и особенностей использования вашего телефона заблокировать и перевыпустить сим-карту;
     c. сменить пароль, воспользовавшись другим доверенным устройством, и/или заблокировать доступ, обратившись в Общество.
   - При подозрении на несанкционированный доступ и/или компрометацию устройства необходимо сменить пароль, воспользовавшись другим доверенным устройством и/или заблокировать доступ, обратившись в Общество, в отношении ключевой информации, если это уместно для Вашей услуги – отозвать скомпрометированный закрытый ключ, в соответствии с правилами, отраженными в договорных и/или процедурных документах.
   - Помните, что наличие резервной копии может облегчить и ускорить восстановление Вашего устройства.

- Лучше всего использовать для финансовых операций отдельное, максимально защищенное устройство, доступ к которому есть только у Вас.
- Контролируйте свой телефон, используемый для получения СМС-кодов. В случае выхода из строя сим-карты, незамедлительно обращайтесь к сотовому оператору для уточнения причин и восстановления связи.
- Регулярно выполняйте резервное копирование важной информации.
- Поддерживайте контактную информацию в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

4. При работе с ключами электронной подписи необходимо:
   - Использовать для хранения секретных ключей электронной подписи внешние носители.
   - Крайне внимательно относиться к ключевому носителю, не оставлять его без присмотра и не передавать третьим лицам, извлекать носители из компьютера, если они не используются для работы.
   - Использовать сложные пароли для входа на устройство и для доступа к ключам электронной подписи, не хранить пароли в текстовых документах на компьютере.
5. При работе на компьютере необходимо:
   - Использовать лицензионное программное обеспечение (операционные системы, офисные пакеты и т.д.);
   - Своевременно устанавливать актуальные обновления безопасности (операционные системы, офисные пакеты и т.д.);
   - Использовать антивирусное программное обеспечение, регулярно обновлять антивирусные базы;
   - Использовать специализированные программы для защиты информации (персональные межсетевые экраны и средства защиты от несанкционированного доступа), средства контроля конфигурации устройств;
   - Использовать сложные пароли;
   - Ограничить доступ к компьютеру, исключить (ограничить) возможность дистанционного подключения к компьютеру третьим лицам.
6. При работе с мобильным устройством необходимо:
   - Не оставлять свое Мобильное устройство без присмотра, чтобы исключить несанкционированное использование;
   - Использовать только официальные Мобильные приложения;
   - Не переходить по ссылкам и не устанавливать приложения/обновления безопасности, пришедшие в SMS-сообщении, Push-уведомлении или по электронной почте, в том числе от имени Общества;
   - Установить на Мобильном устройстве пароль для доступа к устройству.
7. При обмене информацией через сеть Интернет необходимо:
   - Не открывать письма и вложения к ним, полученные от неизвестных отправителей по электронной почте, не переходить по содержащимся в таких письмах ссылкам;
   - Не вводить персональную информацию на подозрительных сайтах и других неизвестных Вам ресурсах;
   - Ограничить посещения сайтов сомнительного содержания;
   - Не сохранять пароли в памяти интернет-браузера, если к компьютеру есть доступ третьих лиц;
   - Не нажимать на баннеры и всплывающие окна, возникающие во время работы с сетью Интернет;
   - Открывать файлы только известных Вам расширений (docx, png, xlsx и т.д.).

При подозрении в компрометации ключей или несанкционированном движении ценных бумаг, денежных средств или иных финансовых активов необходимо незамедлительно обращаться в Общество (тел. +7 (495) 777-29-64, e-mail: depo@region.ru)

Ознакомлен
Клиент: _____

_____ / _____/

М.П.