

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
Микрокредитная компания «ДОСТУКЧА»**

регистрационный номер 208046-3301-ООО; код ОКПО 31553170; ИНН 02207202210377
Кыргызская Республика, город Бишкек, Октябрьский район, улица Горького, 70

ПРИКАЗ № 01-23ОД

город Бишкек

«26» июня 2023 года

Об утверждении Политики информационной безопасности

Руководствуясь пунктом 10.2 Устава Общества с ограниченной ответственностью Микрокредитная компания «ДОСТУКЧА» (далее по тексту – Общество) приказываю утвердить следующее:

1. Политику Информационной безопасности (Приложение №1).
 2. Ознакомить должностных лиц и сотрудников Общества настоящим приказом со всеми приложениями.
 3. Контроль за исполнением настоящего приказа возлагаю на себя.

Приложение на 13 листах:

- ## *1. Политика информационной безопасности.*

Генеральный директор

Д.Ж. Омурбекова



Огнашисас

Микрокредитная компания

Создана по решению

Нормативного акта

Область применения

Сфера и виды

Основные направления

Объекты деятельности

Регионы и города

Классификация избранных целей

УТВЕРЖДЕН

Приказом Генерального директора

ООО МКК «ДОСТУКЧА»

Д.Ж. Омурбековой

№ 01-23 от 26.06.2023 года



ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА с ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «МИКРОКРЕДИТНАЯ КОМПАНИЯ «ДОСТУКЧА»

2023 год

город Бишкек

Кыргызская Республика

Информационная безопасность

Оглавление

Информационная безопасность.....	3
Общие положения.....	3
Нормативные акты.....	4
Область применения.....	4
Цели и задачи	4
Основные свойства	6
Объекты защиты	6
Риск и модель угроз.....	7
Классификация нарушителей	9
Меры обеспечения	11
Сбор, обработка, хранение и передача персональных данных	12
Порядок предоставления информации, содержащей персональные данные.....	13

1.1.2

Политика основана на принципах информационной безопасности, включая основные

1.1.3

цели и задачи, меры по защите информации, являющейся основой

1.1.4

действий Компании по защите информации, служит руководством

1.1.5

в разработке соответствующих документов.

1.1.6

В документе определены должностные полномочия Контролера

1.1.7

и Руководителя по вопросам соблюдения требований информационной

1.1.8

и социальной безопасности, а также требования международных стандартов

1.1.9

установленная Информационной безопасностью.

1.1.10

Политика определяет общие правила деятельности всех работников Компании.

1.1.11

Политика определяет общие правила для лиц, имеющих

1.1.12

доступ к информационным системам и документам Компании, с той целью,

1.1.13

чтобы избежать ущерба от деятельности с Компанией и ее деятельности.

1.1.14

Политика охватывает все информационные системы и документы, генерируемые

1.1.15

и используемыми которых является Компания. Компания обеспечивает создание и

1.1.16

обновление системы управления Информационной безопасностью.

1.1.17

Политика определяет общие правила управления Компанией, прописанные для

1.1.18

важного процессом обеспечения Информационной безопасности. Особенности

1.1.19

информационной безопасности – одна из главнейших функций осуществляемой

1.1.20

действительной деятельности Компании. Информационная безопасность

1.1.21

– состояние технической

1.1.22

и организационных ресурсов, информационных систем и

1.1.23

информационно-коммуникационной инфраструктуры от внешних и внутренних

1.1.24

угроз, которые могут привести к материальному ущербу, нарушить

1.1.25

активность Компании или членов коллектива и/или ущерб Компании, ее

1.1.26

активам, работникам и/или членам

1.1.27

членам семьи членов коллектива Компании. Информационная безопасность

1.1.28

поддается на требования, бывшие разработанные и разработаемые в

1.1.29

согласии с общими принципами правил и нормативными документами в

1.1.30

данной области могут привести к серьезным последствиям, неизвестные

1.1.31

сторонним клиентам и сотрудникам других организаций.

Информационная безопасность

Основной целью обеспечения Информационной безопасности является, прежде всего высокая защищенность интересов Компании, бесперебойное и корректное функционирование системы, своевременное выявление как внешних, так и внутренних угроз, нарушения в работе программных и аппаратных компонентов Информационных систем, а также природные и техногенные катастрофы.

Под Информационной безопасностью Компания понимает комплекс условий, позволяющий предупредить потенциально опасные для Компании действия или обстоятельства, либо минимизация, при котором они не способны причинить ущерб установленной системе функционирования Компании, сохранению и воспроизведству его собственности и инфраструктуры.

Общие положения

- 1.1.1. Политика Информационной безопасности ОсОО МКК «Достукча» определяет цели и принципы обеспечения Информационной безопасности, излагает основные принципы направления и требования по защите информации, является основой для обеспечения режима Информационной безопасности, служит руководством при разработке соответствующих внутренних документов.
- 1.1.2. Нормативно-правовую основу Политики составляют положения Кыргызской Республики по вопросам использования информационных систем и Информационной безопасности, а также требования международных стандартов управления Информационной безопасностью.
- 1.1.3. Положения политики обязательны для исполнения всеми работниками Компании, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам Компании, в той части, которая непосредственно взаимосвязана с Компанией и их деятельностью.
- 1.1.4. Политика охватывает все информационные системы и документы, владельцем и пользователем которых является Компания. Компания обеспечивает создание и функционирование системы управления Информационной безопасностью, являющейся частью общей системы управления Компании, предназначенный для управления процессом обеспечения Информационной безопасности. Обеспечение Информационной безопасности – одно из условий для успешного осуществления кредитной деятельности Компании. Информация, циркулирующая в Компании, является одним из важнейших активов.
- 1.1.5. Информационная безопасность Компании – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации Компании или повлечь нанесения иного ущерба Компании, его учредителям, работникам и/или клиентам.
- 1.1.6. Являясь элементом общей политики Компании, Информационная безопасность основывается на требованиях бизнеса, разрабатывается и реализуется в соответствии с общими правилами управления рисками в Компании. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны клиентов и снижению конкурентоспособности.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ МИКРОКРЕДИТНАЯ КОМПАНИЯ «ДОСТУКЧА»

- 1.1.7. Обеспечение Информационной безопасности включает в себя применение всех доступных средств и инструментов в рамках компетенций работников Компании, направленных на защиту информации и поддерживающей ее инфраструктуры.
- 1.1.8. Неотъемлемой частью организации Информационной безопасности является непрерывный контроль эффективности предпринимаемых мер, определение для работников перечня недопустимых действий (бездействия), возможных последствий и ответственности.
- 1.1.9. В процессе реализации Политики Информационной безопасности в нее могут вноситься изменения и дополнения.

Нормативные акты

- 1.1.10. Политика системы Информационной безопасности в целом основываются на следующих нормативно-правовых актах и международных стандартах (в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания информационной системы Компании в целом, в то же время существует ряд документов, которой либо описывает стратегические аспекты развития Информационной безопасности на государственном уровне, либо регламентирует правила по информационной защите отдельных направлений деятельности):
 - Конституция Кыргызской Республики;
 - Закон КР «Об электронном управлении»;
 - Закон КР «Об информации персонального характера»;
 - Закон КР «Об электронной подписи»;
 - подзаконные акты Кыргызской Республики.

Область применения

- 1.1.11. Политика Информационной безопасности распространяется на всех сотрудников Компании, включая стажеров, контрактников и внешних посетителей (клиенты, технический обслуживающий персонал и т.п.), которые по тем или иным причинам имеют легитимный доступ к Информационной безопасности Компании и его клиентов. Также она применяется в отношении к АРМ персонала Компании, оргтехнике и другим ресурсам информационной структуры Компании.

Цели и задачи

- 1.1.12. Основной целью, на достижение которой направлены все положения Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения и/или сведения их последствий к минимуму.
- 1.1.13. Процесс создания надежной системы информационной защиты является непрерывным. В целях обеспечения достаточно надежной системы Информационной безопасности необходима постоянная регулировка ее параметров, адаптация для отражения новых угроз, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или Политику по мере возникновения такой необходимости. В соответствии с данным положением

определяются следующие этапы цикла управления Информационной безопасности (модель PDCA: Plan-DO-Check-Act)

- Plan - Планирование (разработка) – анализ рисков, определение Политики, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию Информационной безопасности для получения результатов в соответствии с общей стратегией и целями Компании;
 - Do – Реализация (внедрения и эксплуатация) – внедрение и эксплуатация Политики, механизмов контроля, процессов, процедур, программно-аппаратных средств;
 - Check – Проверка (мониторинг и анализ) – оценка, и там где это применимо – измерение характеристик исполнения процессов в соответствии с Политикой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;
 - Act – Корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния Информационной безопасности, требований со стороны руководства, иных факторов в целях обеспечения непрерывного совершенствования системы управления Информационной безопасности;
- 1.1.14. Построение системы управления Информационной безопасности Компании и ее функционирование должно осуществляться в соответствии со следующими основными принципами:
- Законность – любые действия, предпринимаемые для обеспечения Информационной безопасности, осуществляются на основе действующего законодательства с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Компании;
 - Ориентированность на бизнес – Информационная безопасность рассматривается как процесс поддержки основной деятельности Компании. Любые меры по обеспечению Информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Компании;
 - Непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Компании должны осуществляться без прерывания и/или остановки текущих бизнес-процессов Компании;
 - Компетентность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла на всех технологических этапах их использования во всех режимах функционирования;
 - Обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем Информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;
 - Приоритетность – категорирование (ранжирование) всех информационных ресурсов Компании по степени важности при оценке реальных, а также потенциальных угроз Информационной безопасности;
 - Привилегирование – пользователь/сотрудник получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им функциональных обязанностей, либо деятельности в рамках своих полномочий;

- Специализация – эксплуатация технических средств и реализация мер Информационной безопасности должны осуществляться профессионально подготовленным специалистом Компании;
- Информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях Информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер Информационной безопасности;
- Взаимодействие и координация – меры Информационной безопасности на основе взаимосвязи соответствующих структурных подразделений Компании, координация их усилий для достижения поставленных целей, а также установление необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;
- Подтверждаемость - важная документация и все записи – документы, подтверждающие исполнение требований Информационной безопасности системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Основные свойства

- 1.1.15. Информационная безопасность состоит из трех основных компонентов:
 - Конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;
 - Целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);
 - Доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.
- 1.1.16. Политика Информационной безопасности обеспечение Информационной безопасности на основе использования совокупности организационных, режимных, технических, программных и других методов и средств защиты информации, а также осуществления всестороннего непрерывного контроля эффективности реализованных мер по обеспечению Информационной безопасности.

Объекты защиты

- 1.1.17. Основными объектами обеспечения Информационной безопасности в Компании признаются следующие элементы:
 - Информационные ресурсы Компании, его клиентов, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормами документами Компании к банковской коммерческой тайне, персональным данным, финансовой информации, и любой иной информации, необходимой для обеспечения нормального функционирования Компании;

ОБЩЕСТВО с ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ МИКРОКРЕДИТНАЯ КОМПАНИЯ «ДОСТУКЧА»

- Средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
 - Программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Компании, с помощью которых производится обработка защищаемой информации;
 - Процессы Компании, связанные с управление и использованием информационных ресурсов;
 - Помещения, в которых расположены средства обработки защищаемой информации;
 - Рабочие помещения и кабинеты сотрудников Компании, помещения Компании, предназначенные для ведения закрытых переговоров и совещаний;
 - Сотрудники Компании, имеющие доступ к защищаемой информации;
 - Технические средства и системы, обрабатывающие открытую информацию, но размещаемые в помещениях, в которых обрабатывается защищаемая информация;
 - Список пользователей информационных систем Компании, их права и приоритеты на доступ к информации, заведен в матрицы доступов, полномочия к программным и техническим средствам предоставляются в соответствии с матрицами доступов подразделений Компании, процессы регламентированы Правилами допустимого использования информационных ресурсов Компании и Правилами управления логическим доступом к информационным ресурсам Компании.
- 1.1.18. Подлежащая защите информация может:
- Размещаться на бумажных носителях;
 - Существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);
 - Передаваться по телефону, с официальных аккаунтов социальных сетей, сайта Компании и т.п. в виде электрических сигналов;
 - Присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкций во время совещаний и переговоров.

Риск и модель угроз

- 1.1.19. Риски информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов с конкретной угрозой для причинения ущерба Компании. Для управления рисками Информационной безопасности необходимы соответствующие методы определения и обработки рисков, которые могут включать расчет затрат и экономического эффекта, требования законодательных активов, интересы заинтересованных сторон и другие соответствующие данные.
- 1.1.20. Процесс определения рисков, принятый в Компании, включает идентификацию, сравнительную оценку риска, и назначение им приоритетов в соответствии с критериями принятия риска и важностью целей для Компании. Результаты определения рисков Информационной безопасности помогут руководству принять решения относительно управления рисками Информационной безопасности, назначения приоритетов при управлении рисками Информационной безопасности и внедрения соответствующих средств управления безопасностью для защиты от этих рисков.

- 1.1.21. Для оценки риска, процесс определения рисков включает систематический метод оценки величины риска (анализ риска) и процесс сравнивания предполагаемого риска с соответствующими критериями риска. Определение риска должно выполняться периодически, это позволит своевременно учитывать изменения требований Информационной безопасности и возникновение рискованных ситуаций, а также произошедшие существенные изменения. Для определения риска следует использовать методы, обеспечивающие сопоставимые и воспроизводимые результаты.
- 1.1.22. Для эффективного определения риска Информационной безопасности четко определяется область его действия. Определение риска Информационной безопасности будет взаимосвязано с определениями рисков для других областей деятельности (при необходимости). До начала обработки рисков устанавливаются критерии принятия рисков. Риск принимается, если определено, что его уровень низкий или стоимость его обработки для Компании экономически невыгодна, эти критерии документируются.
- 1.1.23. После определения риска для каждого идентифицированного риска должно быть принято решение об его обработке. К возможным опциям обработки рисков относятся:
 - Применение соответствующих средств управления для снижения рисков;
 - Осознанное и объективное принятие рисков, если они однозначно удовлетворяют требованиям и критериям принятия рисков Компании;
 - Разделение совместных рисков с другими сторонами, например, партнерами и/или поставщиками услуг.
- 1.1.24. После принятия решения об обработке рисков используются соответствующие средства управления, которые прежде были выбраны и внедрены. В случаях доступа сторонних организаций к информационным активам Компании и средствам обработки информации необходимого по производственным причинам, а также, в случае получения товаров и услуг от сторонних организаций, проводится анализ рисков для определения возможных последствий для безопасности информации и требований к средствам управления. Такие мероприятия следует согласовать и определять в договорах со сторонней организацией.
- 1.1.25. Все действия по определению, обработке и принятию рисков, обмену информацией относительно рисков, мониторингу рисков, должны выполняться в соответствии со стандартом O'z DSt ISO/IEC 27005:2013
- 1.1.26. Угрозы – под угрозами информационной безопасности понимается совокупность условий и факторов, создающих предпосылки к возникновению инцидента Информационной безопасности.
- 1.1.27. Угрозы информационной безопасности подразделяются на:
 - Случайные – стихийные бедствия (природные источники угроз – землетрясения, пожары, осадки, наводнения и т.п.), непреднамеренные ошибочные действия со стороны работников Компании, ошибки аппаратных и программных средств и т.д.;
 - Преднамеренные, т.е. умышленная фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.п.;
- 1.1.28. К числу угроз Информационной безопасности относятся (но не ограничены ими):
 - Утрата информации, составляющей банковскую тайну, коммерческую тайну Компании и иную охраняемую законом информацию;
 - Искажение (несанкционированная модификация, подделка) защищаемой информации;

- Утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.п.);
 - Несанкционированное использование информационных ресурсов (злоупотребление, мошенничество и т.п.);
 - Недоступность информации в результате ее блокирования, отказа и сбоя оборудования или программ, дезорганизация функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств, и злонамеренных действий.
- 1.1.29. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние Информационной безопасности и его нормальное функционирование:
- Финансовые потери, связанные с утечкой, разглашением, или несанкционированной модификацией защищаемой информации;
 - Финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
 - Финансовые потери, связанные с несанкционированными действиями в информационных ресурсах Компании;
 - Ущерб от дезорганизации деятельности Компании, финансовые и репетиционные потери, связанные с невозможность выполнения им своих обязательств;
 - Ущерб от принятия управленческих решений на основе необъективной информации;
 - Ущерб от отсутствия у руководства компании объективной информации;
 - Ущерб, нанесенный репутации Компании;
 - Иной вид ущерба.

Классификация нарушителей

- 1.1.30. Нарушители Информационной безопасности классифицируются следующим образом:
- Внутренние нарушители – работники Компании, неосознанно либо злонамеренно нарушают режим Информационной безопасности;
 - Внешние нарушители – лица, не связанные с Компанией трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам Компании;
- 1.1.31. Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рискованными категориями следует считать менеджеров высшего и среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.
- 1.1.32. Типы внутренних нарушителей:
- Необученный/халатный работник – сотрудник Компании, по незнанию или по собственной халатности допускающий нарушение, не несущее в себе злого умысла;
 - Конкурирующий работник – сотрудник Компании, по личной неприязни либо по иным причинам пытающийся нанести ущерб другому работнику. В результате его действий может пострадать не только его «цель», но и Компания в целом;

- Заинтересованный нарушитель – сотрудник Компании, который заинтересован в неправомерных действиях по отношению к Компании третьей стороной либо собственной выгодой. Как правило, заинтересован в дальнейшем сохранении с Компанией трудовых отношений и не будет предпринимать действий, прямо его компрометирующих. Наиболее вероятное нарушение – утечка информации (в случае заинтересованности собственной выгодой – финансовые мошенничества);
- Внедренный злоумышленник – сотрудник Компании, поступивший на работу с целью совершения противоправных действий в интересах третьих лиц. Практически не заинтересован в дальнейших трудовых отношениях с Компанией;
- Увольняющийся сотрудник – сотрудник Компании, прекращающий с Компанией трудовые отношения без взаимных претензий. Наиболее вероятна утечка информации, к которой он имел доступ;
- Обиженный сотрудник – сотрудник Компании, неудовлетворенный условиями трудовой деятельности, либо, как вариант, руководство Компании явно недовольно деятельностью работника. Возможны любые, даже самые нелогичные нарушения, особенно в момент расторжения трудовых отношений;

1.1.33. Основные типы внешних нарушителей

- «Script Kiddie», или «Начинающий» - лицо, интересующееся взломом любого информационного ресурса, имеющего общеизвестные уязвимости. Не нацелен на взлом информационных ресурсов именно Компании, легко прекращает атаку в случае обнаружения серьезных средств защиты. Как правило, использует широко распространенные методы взлома, не разрабатывает собственных средств;
- «Black hat», или «Черный хакер» - в отличие от «Script Kiddie» более упорен во взломе конкретного ресурса, обход систем защиты считает «делом чести», может разрабатывать простые атакующие средства. Действует с целью самоутверждения или для извлечения выгоды, может продавать свои услуги криминальным структурам;
- «Elite hacker», или «Гуру» - высококлассный специалист по взлому информационных систем. Как правило, работает «под заказ» криминальных структур либо конкурирующих организаций. В первом случае будет нацелен на проведение финансового мошенничества, во втором – либо на утечку информации, либо на недоступность серверов и компрометацию Компании в глазах клиентов. В арсенале имеет полный спектр специального программно-технического обеспечения, а также использует методы социальной инженерии;
- «Партнер» - работник организации – партнера, имеющих доступ к информационной системе Компании. Можно определить любым типом внутреннего нарушителя, но он, как правило, менее управляем и менее осведомлен о требованиях Информационной безопасности, принятых в Компании;
- «Консультант» - работник сервисной компании, который имеет доступ к информационным ресурсам. Возможны разные сценарии проявления несанкционированной деятельности, как правило, в рамках обслуживаемой информационной системы;
- «Стажер/практиканта» - как правило, ограничен в доступе к информации и информационным системам, однако постоянно находится на территории Компании и может получать информацию косвенно либо методами социальной инженерии. Может нанести серьезный ущерб только при халатном отношении к своим обязанностям работника Компании, курирующего данного стажера/практиканта;
- «Клиент» - клиент Компании, имеющий доступ к его сервисам дистанционного обслуживания. Может нанести урон при неправильном использовании данных

ресурсов, утере идентификационных данных либо действовать как первые три типа внешних нарушителей, имея – пусть и ограниченный доступ к информационным ресурсам.

Меры обеспечения

- 1.1.34. Основными мерами по обеспечению Информационной безопасности Компании являются:
 - Административно – правовые и организационные меры;
 - Меры физической безопасности;
 - Программно-технические меры;
- 1.1.35. Административно – правовые и организационные меры включают, но не ограничены ими:
 - Контроль исполнения требований Законодательства Кыргызской Республики и внутренних процедур Компании;
 - Разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
 - Контроль соответствия бизнес-процессов требованиям Политики;
 - Информирование и обучение работников Компании работе с информационными ресурсами и требованиями Информационной безопасности;
 - Реагирование на инциденты, локализацию и минимизацию последствий;
 - Анализ новых рисков Информационной безопасности;
 - Отслеживание и улучшение морально-делового климата в коллективе;
 - Определение действий при возникновении чрезвычайных ситуаций;
 - Проведение профилактических мер при приеме на работу и увольнении работников Компании;
 - Организация и обеспечение системой поддержания заданных параметров температуры и влажности;
 - Обеспечение системой видеонаблюдения;
 - Морально-этические (психологические меры);
- 1.1.36. Меры физической безопасности включают, но не ограничены ими:
 - Организацию пропускного и внутри объектного режимов;
 - Построение периметра безопасности защищаемых объектов;
 - Организацию круглосуточной охраны режимных объектов, в том числе с использованием технических средств безопасности;
 - Организацию противопожарной безопасности охраняемых объектов;
 - Контроль доступа сотрудников Компании в помещения ограниченного доступа.
- 1.1.37. Программно-технические меры включают, но не ограничены ими:
 - Использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
 - Использование средств защиты периметра (firewall, Intrusion Prevention System (IPS) и т.п.);
 - Применение комплексной антивирусной защиты
 - Использование средств ИБ, встроенных в информационные системы;

- Использование специальных комплексов ИБ (как защита электронных информационных ресурсов, так и защита от утечки по электромагнитным и акустическим каналам);
- Обеспечение регулярного резервного копирования информации;
- Контроль за правами и действиями пользователей, в первую очередь привилегированных;
- Применение систем криптографической защиты информации;
- Обеспечение безотказной работы аппаратных средств;
- Мониторинг состояния критичных элементов информационной системы.

Сбор, обработка, хранение и передача персональных данных

- 1.1.38. Сбор, обработка, хранение и передача персональных данных (далее по тексту – «обработка персональных данных») клиентов Компании осуществляется исключительно для соблюдения законов и иных нормативных правовых актов, соответствия целям, заранее определенным и заявленным при сборе персональных данных.
- 1.1.39. Объем и содержание и способы обработки персональных данных клиентов Компании, соответствуют требованиям законодательства и другим нормативным актам и целям обработки. Не допускается обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных.
- 1.1.40. Персональные данные Компания получает только у самого клиента.
- 1.1.41. При обработке персональных данных обеспечивается точность, их достаточность, а в необходимых случаях актуальность по отношению к целям обработки персональных данных. Компанией принимаются необходимые меры по уничтожению/удалению либо уточнению неполных и/или неточных данных.
- 1.1.42. Обработка персональных данных субъектов персональных данных проводится с целью выполнения кредитных операций, повышения оперативности и качества обслуживания клиентов, установленного правилами Кредитора, а также исполнения норм действующего законодательства Национального банка Кыргызской Республики.
- 1.1.43. Компания обрабатывает следующие категории персональных данных клиентов:
 - Информация, связанная с непосредственным оказанием услуг, что среди прочего включает соглашения, заявку, кредитный договор и т.д.;
 - Фото, видео, фамилия, имя, отчество, гражданство, год и месяц, дата и место рождения, реквизиты документа удостоверяющего личность гражданина, ИИН, сведения о регистрации по месту жительства или временной регистрации по месту пребывания, о месте проживания, данные сведения о семейном положении, месте работы, сведения о ежемесячных расходах и доходах, образование, номера мобильного, домашнего, рабочего телефонов, адрес электронной почты, реквизиты банковского счета, а также иные данные, которые могут передаваться автоматически в процессе использования мобильного приложения;
 - Компания имеет право проверять достоверность персональных данных, предоставляемых клиентом;
 - Клиенту дается право в любое время внести изменения ранее представленные персональные данные через личный кабинет в мобильном приложении, либо обративших в информационный центр Компании.
- 1.1.44. Обработка персональных данных в Компании осуществляется путем сбора, систематизации, накопления, хранения, уточнения (обновления, изменения) использования, передачи (предоставления доступа), обезличивания,

- блокирования, уничтожения персональных данных исключительно для обеспечения соблюдения утвержденного процесса кредитования.
- 1.1.45. Передача персональных данных третьим лицам осуществляется только в соответствии с действующим законодательством, в том числе с использованием защищенных телекоммуникационных каналов связи.
- 1.1.46. Трансграничная передача персональных данных (передача персональных данных на территорию иностранного государства) осуществляется только в случае обеспечения этими государствами защиты персональных данных. Трансграничная передача персональных данных на территорию иностранных государств может быть запрещена или ограничена закона Кыргызской Республики.
- 1.1.47. Сроки хранения документов, содержащих персональные данные клиентов определяются датой достижения целей их сбора и обработки, если иное не предусмотрено законодательством Кыргызской Республики. По истечению сроков хранения таких документов они подлежать уничтожению.
- 1.1.48. С целью защиты персональных данных при обработке в информационных системах персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий с ними Компанией применяются организационные и технические меры в соответствии с Политикой безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса, мобильного приложения.

Порядок предоставления информации, содержащей персональные данные

- 1.1.49. При обращении субъекта персональных данных или получении запроса Компания безвозмездно предоставляет в сроки, предусмотренные законодательством Кыргызской Республики, персональные данные, относящиеся к субъекту персональных данных, в доступной форме, исключающей предоставление персональных данных, относящихся к другим субъектам персональных данных.
- 1.1.50. Сторонние организации имеют право доступа к персональным данным субъектов персональных данных только, если они наделены необходимыми полномочиями в соответствии с законодательством Кыргызской Республики, либо на основании заключения партнерских договоров и соглашений заключенных с Компанией.
- 1.1.51. При передаче персональных данных клиентов Компания и уполномоченные должностные лица соблюдают следующие правила:
- Не сообщают персональные данные третьей стороне без письменного согласия клиента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью клиента, а также в случаях, установленных законодательством Кыргызской Республики;
 - Предупреждают лиц, получающих персональные данные, о том, что эти данные могут быть использованы только в целях, для которых они сообщены и требуют от этих лиц подтверждения соблюдения этого условия, за исключением случаев, установленных законодательством;
 - Не отвечают на вопросы, связанные с предоставлением персональной информации, любым третьим лицам без законных оснований;
 - Ведут учет передачи персональных данных клиента по поступившим в Компанию запросам.

Прошито, пронумеровано и скреплено

Печатью 13 (три надиза) листов

Должность Ген. dir.

Подпись

