«УТВЕРЖДЕНО»
Решением Единственного участника
ТОО «МФО «FinFix»
Приказ №____
от «__» _____ 2025 года

Политика информационной безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса

г. Алматы

1.Общие положения

1.1 Настоящая Политика информационной безопасности и защиты информации от несанкционированного доступа при предоставлении услуг через интернет-ресурс (веб-сайт) ТОО «Микрофинансовая организация «FinFix» (далее — Политика), разработана в соответствии с требованиями действующего законодательства Республики Казахстан в области информационной безопасности, нормативными актами уполномоченного государственного органа, а также внутренними документами ТОО «МФО «FinFix» (далее — МФО) и носит рекомендательный характер.

Пользователям рекомендуется ознакомиться с документом для исключения негативных ситуаций, связанных с информационной безопасностью, мошенничеством и иными инцидентами.

1.2. Целью настоящей Политики является минимизация ущерба от инцидентов, представляющих угрозу информационной безопасности, путём их предотвращения либо снижения последствий до приемлемого уровня. Обеспечение информационной безопасности не является самоцелью, а представляет собой необходимую меру по управлению рисками и снижению возможных экономических потерь, связанных с угрозами в отношении информационных ресурсов МФО.

2. Основные принципы Политики

Настоящая Политика основывается на следующих ключевых принципах:

- Законность — все действия, направленные на обеспечение информационной безопасности, осуществляются в строгом соответствии с действующим законодательством Республики Казахстан. Применяются все предусмотренные законом методы выявления, предотвращения, локализации и нейтрализации негативных воздействий на объекты защиты информации МФО.
- Ориентированность на бизнес — информационная безопасность рассматривается как инструмент поддержки основной деятельности МФО. Реализация мер защиты не должна создавать значительных препятствий для функционирования бизнес-процессов.
- Непрерывность — обеспечение информационной безопасности осуществляется без прерывания или остановки текущих бизнес-процессов. Все меры должны быть интегрированы в повседневную деятельность организации.
- Комплексность — защита информации охватывает все этапы жизненного цикла информационных ресурсов, включая их создание, обработку, хранение, передачу и уничтожение, а также все режимы функционирования соответствующих систем.
- Обоснованность и экономическая целесообразность — используемые средства и методы защиты должны соответствовать актуальному уровню развития науки и техники, быть экономически оправданными и адекватными установленному уровню риска. Затраты на реализацию мер информационной безопасности не должны превышать потенциальный ущерб от реализации соответствующих угроз.
- Приоритетность — информационные ресурсы подлежат ранжированию по степени их значимости и чувствительности. Это позволяет сосредоточить ресурсы на защите наиболее критичных активов с учетом оценки как существующих, так и потенциальных угроз.

3. Содержание Политики

Настоящая Политика устанавливает:

- основные меры обеспечения информационной безопасности МФО, включая минимизацию и предотвращение угроз;
- порядок двухфакторной аутентификации и верификации заемщиков через интернет-ресурс;
- правила безопасного хранения электронных сообщений и документов, с обеспечением их целостности и конфиденциальности в течение не менее 5 лет после завершения договорных обязательств;
- меры по предотвращению возможных противоправных действий со стороны третьих лиц.

4. Объекты действия Политики

Политика распространяется на:
- сотрудников МФО, включая стажеров и практикантов;
- заемщиков и иных лиц, имеющих доступ к информационным системам МФО;
- контрагентов и партнеров, взаимодействующих с МФО по договорным основаниям;
- информационные ресурсы МФО — базы данных, системную документацию, руководства, политики и процедуры, включая как конфиденциальную, так и общедоступную информацию.

5. Информационная инфраструктура

К объектам защиты относятся:
- IT-системы МФО, средства обработки, хранения, передачи и отображения информации;
- каналы связи, телекоммуникационные системы, информационные носители;
- технические и программные средства защиты;
- помещения и объекты, где размещены элементы IT-инфраструктуры.

6. Настоящая Политика является общедоступным документом и размещается на официальном Интернет-ресурсе МФО https://kopaksha.kz/.

7. Процесс создания надежной системы информационной защиты

Процесс создания надежной системы информационной безопасности не является завершённым действием. Для поддержания достаточного уровня защиты необходима постоянная настройка параметров системы, а также её адаптация к новым угрозам, возникающим как во внешней, так и во внутренней среде.

8. Меры обеспечения информационной безопасности

8.1. Основными мерами обеспечения информационной безопасности МФО являются:
- административно-правовые и организационные меры;
- меры физической безопасности;
- программно-технические меры.

8.2. Административно-правовые и организационные меры включают (но не ограничиваются перечисленным):
- контроль соблюдения требований законодательства РК и внутренних нормативных документов;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику информационной безопасности;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение сотрудников МФО по вопросам работы с информационными системами и соблюдения требований информационной безопасности;

- реагирование на инциденты, локализация и минимизация их последствий;
- анализ новых рисков в области информационной безопасности;
- мониторинг и улучшение морально-делового климата в коллективе;
- определение порядка действий в случае возникновения чрезвычайных ситуаций;
- проведение профилактических мероприятий при приёме на работу и увольнении сотрудников.

8.3. Меры физической безопасности включают (но не ограничиваются):

- организацию круглосуточной охраны охраняемых объектов, включая использование технических средств безопасности;
- обеспечение противопожарной безопасности охраняемых объектов;
- контроль доступа сотрудников МФО и третьих лиц в помещения с ограниченным доступом (например, серверные комнаты).

8.4. Программно-технические меры включают (но не ограничиваются):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- применение средств защиты периметра (межсетевые экраны и др.);
- использование комплексной антивирусной защиты;
- анализ исходного кода, компонентов и библиотек с применением инструментов статического анализа, поддерживающих все используемые языки программирования;
- использование встроенных средств информационной безопасности в информационных системах;
- регулярное резервное копирование данных;
- контроль прав доступа и действий пользователей, особенно привилегированных;
- применение систем криптографической защиты информации;
- обеспечение бесперебойной работы аппаратных средств.

9. Оценка рисков информационной безопасности

9.1 Для оценки рисков информационной безопасности микрофинансовой организацией (МФО) проводятся следующие мероприятия:

- формирование перечня критичных информационных активов;
- оценка рисков информационной безопасности для критичных информационных активов.

9.2. В перечень критичных информационных активов включаются те активы, убытки от нарушения конфиденциальности, целостности или доступности которых превышают установленный уровень существенности потерь, связанных с инцидентами информационной безопасности.

9.3. В целях проведения оценки рисков информационной безопасности в отношении критичных информационных активов МФО обеспечивает реализацию следующих процессов:

- идентификация угроз информационной безопасности;
- определение источников угроз, релевантных для каждого критичного актива;
- выявление уязвимостей критичных информационных активов;
- анализ существующих мер управления рисками информационной безопасности;
- оценка вероятности реализации угроз со стороны соответствующих источников;

- оценка общего уровня рисков информационной безопасности.

9.4. Идентификация угроз информационной безопасности в отношении критичных информационных активов осуществляется подразделением по информационной безопасности. Для каждого такого актива проводится анализ потенциальных угроз.

9.5. Идентификация релевантных источников угроз осуществляется также подразделением по информационной безопасности с учетом известных и потенциальных источников угроз.

9.6. Выявление уязвимостей критичных информационных активов проводится подразделением по информационной безопасности МФО с учетом следующей информации:

- конструктивные особенности информационного актива;
- физическое расположение актива;
- известные ошибки в программном обеспечении;
- ошибки конфигурации;
- недостатки в процессе эксплуатации актива.

9.7. Идентификация существующих мер управления рисками осуществляется подразделением по информационной безопасности с учетом как организационных, так и технических мероприятий, направленных на устранение уязвимостей и минимизацию последствий возможных инцидентов.

9.8. Оценка вероятности реализации угроз информационной безопасности в отношении критичных информационных активов осуществляется подразделением по информационной безопасности. Анализ проводится для всех релевантных комбинаций: источник угрозы – угроза – уязвимость, с учетом следующей информации:

- данные о расположении источника угрозы по отношению к критичному информационному активу (внутренний или внешний). Для внутренних источников учитывается количество пользователей, имеющих доступ к активу; для внешних — возможность удаленного доступа извне периметра защиты;
- уровень доступа, которым обладает источник угрозы;
- статистические данные о частоте реализации аналогичных угроз в прошлом;
- информация о сложности реализации конкретной угрозы для данного актива;
- наличие защитных мер, реализованных в отношении рассматриваемого информационного актива.

9.9. В случае привлечения нескольких экспертов к оценке вероятности реализации угрозы и получения различных оценок, итоговая (обобщенная) оценка принимается равной наибольшей из представленных, то есть отражающей максимальную вероятность реализации угрозы.

9.10. Оценка уровня рисков информационной безопасности осуществляется путем сопоставления:

- оценок вероятности реализации угроз критичным информационным активам со стороны источников угроз,
- и оценок потенциальных убытков, связанных с нарушением конфиденциальности, целостности или доступности этих активов.

10. Требования к автоматизированной информационной системе

10.1. Автоматизированная информационная система включает в себя:

- программное обеспечение серверов веб-приложений (далее — веб-приложение);
- программное обеспечение серверов программных интерфейсов (далее — серверное ППО).

10.2. Разработка и/или доработка автоматизированной информационной системы осуществляется МФО в соответствии с внутренним документом, регламентирующим порядок, этапы разработки и состав участников.

10.3. Хранение исходных кодов автоматизированной информационной системы, разрабатываемой в МФО, осуществляется в специализированных системах управления репозиториями кода, размещенных внутри периметра защиты МФО с обязательным обеспечением резервного копирования.

10.4. Обязательным этапом разработки является тестирование безопасности, в рамках которого проводятся, как минимум, следующие мероприятия:
- статический анализ исходного кода;
- анализ компонентов и сторонних библиотек.

10.5 Статический анализ исходного кода проводится с использованием специализированного сканера, поддерживающего все языки программирования, применяемые в анализируемом программном обеспечении. Сканер должен выявлять, в том числе, следующие уязвимости:
- наличие механизмов, допускающих инъекции вредоносного кода;
- использование уязвимых операторов и функций языков программирования;
- использование слабых или уязвимых криптографических алгоритмов;
- наличие кода, способного привести к отказу в обслуживании или замедлению работы приложения;
- возможность обхода механизмов защиты приложения;
- использование секретов (паролей, ключей и т.п.) в открытом виде;
- несоблюдение шаблонов и практик безопасной разработки.

10.6. Анализ компонентов и сторонних библиотек осуществляется с целью выявления известных уязвимостей в используемых версиях, а также для отслеживания их зависимостей.

10.7. МФО обязуется устранять выявленные уязвимости в соответствии с внутренним регламентом. При этом критичные уязвимости устраняются до ввода автоматизированной информационной системы (или ее новых версий) в эксплуатацию.

10.8. МФО обеспечивает хранение всех версий исходных кодов и результатов тестирования безопасности автоматизированной информационной системы, введённых в эксплуатацию за последние три (3) года, с возможностью оперативного доступа к ним.

10.9. Передача данных между клиентской и серверной сторонами автоматизированной информационной системы шифруется с использованием протокола Transport Layer Security (TLS) версии не ниже 1.2.

10.10. Веб-приложение должно обеспечивать:
- однозначную идентификацию принадлежности МФО (доменное имя, логотип, фирменные цвета);

- запрет на сохранение авторизационных данных в браузере;
- маскирование вводимых секретных данных (например, паролей);
- информирование пользователя на странице авторизации о правилах кибербезопасности;
- безопасную обработку ошибок — без отображения конфиденциальной информации, с предоставлением минимально необходимого описания ошибки.

10.11. МФО на стороне серверного ППО обеспечивает:
- безопасную обработку ошибок и исключений — без раскрытия конфиденциальной информации, с возможностью диагностики;
- идентификацию и аутентификацию пользователей и устройств;
- проверку входных данных на валидность для предотвращения инъекций и атак с подделкой запросов.

10.12. Доступ к информации в автоматизированной информационной системе предоставляется сотрудникам МФО в пределах, необходимых для выполнения ими служебных обязанностей с использованием процедур идентификации и аутентификации работников МФО.

10.13. В системе реализуются функции управления учетными записями и паролями, а также блокировки учетных записей в соответствии с внутренними документами МФО.

10.14. Автоматизированная информационная система сопровождается технической поддержкой, включающей предоставление обновлений, в том числе по безопасности.

10.15. Система обеспечивает регулярное резервное копирование данных, файлов и настроек, необходимое для восстановления работоспособной копии.

10.16. В МФО обеспечивается ведение и защита аудиторского следа автоматизированной информационной системы как на организационном, так и на техническом уровне.

10.17. Для защиты системы используется лицензионное антивирусное программное обеспечение или решения для контроля целостности программной среды на рабочих станциях, ноутбуках и мобильных устройствах.

10.18. МФО обеспечивает безопасное хранение электронных сообщений и иных документов, переданных клиенту и полученных от него, с сохранением их целостности и конфиденциальности не менее пяти (5) лет после завершения обязательств по договору микрокредита. Документы хранятся в том виде, в котором были сформированы, отправлены или получены.

11. Безопасное хранение электронных сообщений и иных документов

11.1. В целях обеспечения информационной безопасности МФО выполняются следующие условия:
- организация системы управления информационной безопасностью;
- организация доступа к информационным активам;
- обеспечение безопасности информационной инфраструктуры;
- проведение мониторинга деятельности по обеспечению информационной безопасности, выявление и анализ угроз, противодействие атакам, расследование инцидентов;
- анализ информации об инцидентах информационной безопасности, включая данные о нарушениях и сбоях в информационных системах;
- использование средств криптографической защиты информации;

- обеспечение информационной безопасности при доступе третьих лиц к информационным активам;
- проведение внутренних проверок состояния информационной безопасности;
- реализация процессов системы управления информационной безопасностью.

11.2. Защищаемая информация может:

- размещаться на бумажных носителях;
- существовать в электронном виде (обрабатываться, передаваться, храниться с использованием средств вычислительной техники, записываться и воспроизводиться с помощью технических средств);
- передаваться по телефонной связи, факсу, телексу и другим средствам связи в виде электрических сигналов;
- восприниматься в виде акустических и вибрационных сигналов в воздушной среде и ограждающих конструкциях (например, во время совещаний и переговоров).

11.3. В части обеспечения информационной безопасности при взаимодействии с кредитным бюро (КБ) по договорам на предоставление сведений о потенциальных заемщиках (включая данные о доходах, перечислениях из ГФСС, пенсионных выплатах, кредитных отчетах и т. п.) МФО руководствуется следующими требованиями:

11.3.1. МФО обеспечивает конфиденциальность и целостность информации, получаемой из информационной системы КБ.

11.3.2. МФО соблюдает условия информационной безопасности в соответствии с заключёнными договорами с КБ.

11.3.3. МФО реализует организационно-технические и технологические меры, необходимые для функционирования и защиты программного обеспечения, используемого при взаимодействии с информационной системой КБ.

11.3.4. Оборудование, применяемое для работы с системой КБ, должно быть защищено от несанкционированного доступа. Также обеспечивается защита используемых носителей информации и сетевых ресурсов.

11.3.5. МФО определяет и утверждает перечень ответственных лиц, участвующих во взаимодействии с информационной системой КБ.

11.3.6. Ответственные лица подписывают обязательства о неразглашении и нераспространении информации, ставшей им известной в процессе выполнения своих обязанностей.

11.3.7. МФО разрабатывает и утверждает внутренние документы, устанавливающие порядок назначения ответственных лиц, их права, обязанности и ответственность (в том числе через должностные инструкции).

11.3.8. Доступ к информации предоставляется работникам МФО в объеме, необходимом для исполнения их функциональных обязанностей.

11.3.9. Учетная запись в информационной системе КБ привязана к конкретному физическому лицу.

11.3.10. МФО проводит плановые и внеплановые проверки соответствия рабочих станций и сайта требованиям настоящей Политики информационной безопасности.

11.3.11. По запросу уполномоченного органа МФО предоставляет сведения, подтверждающие соблюдение требований, предусмотренных договорами с КБ.

11.3.12. Операционная система рабочей станции обеспечивает:
- идентификацию и аутентификацию пользователя;
- разграничение прав доступа пользователей;
- авторизацию в соответствии с назначенными правами.

11.3.13. Для взаимодействия с информационной системой КБ используется исключительно рабочая станция, принадлежащая МФО.

11.3.14. При подключении к системе КБ одновременный доступ к другим интернет-ресурсам не допускается.

11.3.15. Работники МФО обязаны обеспечивать конфиденциальность персональных идентификационных и аутентификационных данных, используемых при доступе к информационным системам.

11.3.16. Работники МФО обязаны соблюдать конфиденциальность информации, полученной в ходе работы с информационной системой КБ.

11.4. Ответственность за обеспечение информационной безопасности возлагается на все структурные подразделения МФО в рамках их полномочий и в соответствии с настоящей Политикой и связанными внутренними документами.

11.5. За нарушение требований настоящей Политики и связанных с ней документов предусмотрена ответственность в соответствии с внутренними нормативными актами МФО и действующим законодательством Республики.

12.Меры профилактики нарушений информационной безопасности

12.1. Важную роль в профилактике инцидентов кибербезопасности играет соблюдение национальных и международных требований при разработке программного обеспечения, проектировании компонентов информационных систем и инфраструктуры финансового сектора.
МФО проводит регулярную оценку рисков кибербезопасности, которая служит основой для разработки и внедрения мер по их минимизации, а также для оценки эффективности реализованных защитных мер.

12.2. Учитываются результаты, полученные на этапе профилактики (предотвращения), а также опыт обработки уже произошедших инцидентов. Своевременно проводится оценка характера, масштаба и последствий инцидентов кибербезопасности. В целях минимизации последствий:
- осуществляется оперативное информирование заинтересованных сторон;
- координируются действия по реагированию.

К заинтересованным сторонам относятся:
- Национальный Банк Республики Казахстан;
- иные уполномоченные государственные и законодательные органы;

- заемщики;
- кредиторы и инвесторы;
- работники структурных подразделений МФО;
- поставщики услуг.

12.3. После инцидента обеспечивается непрерывность операционной деятельности МФО параллельно с выполнением процедур восстановления, включая:
- устранение последствий инцидента;
- восстановление нормального функционирования информационных систем и данных с подтверждением их корректности;
- выявление и устранение уязвимостей, использованных в ходе инцидента, для предотвращения повторных инцидентов;
- организацию информационного взаимодействия внутри страны и при необходимости — за ее пределами.

12.4. Повышение осведомленности пользователей и квалификации работников МФО способствует снижению рисков и формированию культуры информационной безопасности. В рамках обучающих мероприятий следует использовать реальный опыт профилактики и реагирования, чтобы сотрудники понимали актуальные угрозы и методы их предотвращения.

12.5. Классическая модель информационной безопасности основывается на обеспечении следующих атрибутов:

- Доступность — обеспечение возможности своевременного и беспрепятственного доступа к информации для уполномоченных лиц;
-Конфиденциальность — ограничение доступа к информации только для лиц, обладающих соответствующими полномочиями, а также предотвращение её раскрытия неавторизованным субъектам;
- Целостность — сохранение информации в неизменном и достоверном виде, исключающем её искажение или несанкционированное изменение.

12.6. В случае выявления несанкционированного доступа, изменения информации, связанной с микрокредитованием, или иных неправомерных действий со стороны третьих лиц, МФО:

- незамедлительно принимает меры по устранению причин и последствий;
- в течение одного рабочего дня уведомляет об этом уполномоченный государственный орган.

12.7. МФО предпринимает меры по недопущению использования своих сервисов и технологий микрокредитования в целях:
- легализации (отмывания) доходов, полученных преступным путем;
- финансирования терроризма.

При предоставлении микрокредитов и проведении скоринга заемщиков, МФО руководствуется:

- Законом Республики Казахстан от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Закон о ПОДФТ);

13. Порядок внесения изменений в Политику

13.1. Предложения по внесению изменений и дополнений в настоящую Политику могут быть инициированы любым сотрудником МФО посредством подачи письменного обращения директору МФО.

13.2. Изменения и дополнения в Политику вносятся:
- при внесении изменений в законодательство Республики Казахстан;
- по мере необходимости, в случае выявления несоответствий, пробелов или необходимости актуализации положений.