Утверждено
Единственным Участником
ТОО «МФО «SM-INVEST»
_____ Акулова Д.А.
Решение №9 от «14» мая 2021 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА В ТОО «МФО «SM INVEST»

Алматы 2021 г.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса в ТОО «МФО «SM INVEST» (далее - Политика) разработана в соответствии с нормами действующего законодательства Республики Казахстан в сфере информационной безопасности, Актами уполномоченного органа и внутренними документами ТОО «МФО «SM INVEST» (далее - МФО).

2. Основной целью Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму. Информационная безопасность необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам МФО. С этой целью необходимо поддерживать главные свойства информации, а именно:

- доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;
- конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) 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).

3. Основными принципами Политики являются:

- 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 МФО;
- ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности МФО;
- непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты МФО должны осуществляться без прерывания или остановки текущих бизнес-процессов МФО;
- комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и 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.

4. Настоящая Политика определяет:

- основные меры по обеспечению информационной безопасности МФО;
- способы многофакторной аутентификации и верификации потенциальных заемщиков посредством интернет-ресурса;
- обеспечение безопасного хранения электронных сообщений и иных документов, предоставленных заемщику и полученных от него, с соблюдением их целостности и

конфиденциальности в течение не менее 5 (пяти) лет после прекращения обязательств сторон по договору о предоставлении микрокредита;

- меры для профилактики предполагаемых правонарушений со стороны третьих лиц.

5. Настоящая Политика обязательна для исполнения всеми работниками МФО, стажерами, практикантами, в той их части, которая непосредственно взаимосвязана с МФО и их деятельностью.

6. Процесс создания надежной информационной защиты никогда не бывает законченным. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды.

7. Область применения: Политика распространяется на всех работников МФО.

ГЛАВА 2. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8. Основными мерами по обеспечению информационной безопасности МФО являются:

- административно-правовые и организационные меры;
- меры физической безопасности;
- программно-технические меры.

8.1. Административно-правовые и организационные меры включают (но не ограничены ими):

- контроль исполнения требований законодательства РК и внутренних документов;
- разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
- контроль соответствия бизнес-процессов требованиям Политики;
- информирование и обучение работников МФО работе с информационными системами и требованиям информационной безопасности;
- реагирование на инциденты, локализацию и минимизацию последствий; анализ новых рисков информационной безопасности;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников МФО.

8.2. Меры физической безопасности включают (но не ограничены ими):

- организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
- контроль доступа работников МФО в помещения ограниченного доступа (сервер).

8.3. Программно-технические меры включают (но не ограничены ими):

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра;
- применение комплексной антивирусной защиты;
- использование средств информационной безопасности, встроенных в информационные системы;
- обеспечение регулярного резервного копирования информации;
- контроль за правами и действиями пользователей;
- обеспечение безотказной работы аппаратных средств.

ГЛАВА 3. БИЗНЕС-ПРОЦЕСС АУТЕНТИФИКАЦИИ, МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ЧЕРЕЗ ДОСТУП ИНТЕРНЕТ-РЕСУРСА ПОСРЕДСТВОМ РЕГИСТРАЦИИ НА САЙТЕ МФО ДЛЯ ВХОДА В ЛИЧНЫЙ КАБИНЕТ И ПОЛУЧЕНИЯ МИКРОКРЕДИТА

9. Идентификации и аутентификации клиента в личном кабинете клиента используются следующие способы:

1) электронная цифровая подпись, представленная национальным удостоверяющим центром Республики Казахстан;

2) биометрическая идентификация посредством использования услуг ЦОИД;

3) двухфакторная аутентификация.

Двухфакторная аутентификация осуществляется путем применения следующих двух параметров:

генерации и ввода паролей или использованием не менее одного из аутентификационных признаков (токенов, смарт-карт, одноразовых паролей).

10. Бизнес-процесс аутентификации, двухфакторная аутентификации и верификации посредством регистрации через сайт МФО для входа в личный кабинет, осуществляется следующим образом:

10.1. В диалоговом окне запрашивает номер телефона потенциального заемщика, для отправки sms-сообщения с уникальным кодом, который действует в течение 1-ой минуты. Код в свою очередь вводится в ячейку Пароль, тем самым активирует личный кабинет к дальнейшей работе. Данное действие подтверждает, что заемщик имеет при себе данный номер и имеет полный доступ к нему.

После регистрации на сайте МФО, через зарегистрированный личный кабинет потенциального клиента и проведения всех процедур и ознакомления всех документов на получение микрокредита в электронном виде и подписание сопутствующих документов клиентом, более детальная процедура расписано в правилах микрокредитования и тп.

10.2. После прохождения этапных процедур заполнения анкетных данных для оформления микрокредита в личном кабинете, потенциальному заемщику необходимо произвести следующие действия:

1) загрузить фотографию в анфас на светлом фоне, с нейтральным выражением лица и закрытым ртом с документом удостоверяющую личность потенциального клиента в формате jpg, gif, png. Для сравнения или сличения биометрии лица (фото) клиента среди биометрии (фото) с другими вложенными документами удостоверяющей личности клиента, также требуется направить взгляд на камеру фотографирующего устройства. При этом, необходимо снять очки и головной убор;

2) загрузить сфотографированный документ, удостоверяющий личность Заявителя, при этом необходимо соблюдения требования прикрепления документа в случае, если это - Паспорт-фотография основной страницы, Удостоверение личности – фотография с обеих сторон, производится биометрия номера ИИН, ФИО и тд;

3) Загрузить фотографию лицевой стороны банковской карты.

В момент подтверждения клиентом о получения микрокредита, система автоматический направляет заявку верификатору на проверку его подлинности, соответствии и распознавание ключевых данных, таких как биометрия лица, ИИН, ФИО и других данных. Это служит дополнительным доказательством того, что прошедший идентификацию заемщик, получил запрашиваемые средства. Верификатор имеет право в случае сомнения дополнительно произвести проверку или отказать.

Сомнительные заявки, не прошедшие ручную верификацию, вносится автоматически в черный список, и в последующем при повторном обращении данного лица в МФО, система сразу же отображает в личном кабинете отказ в оформлении микрокредита.

Кроме того, руководитель на еженедельной основе производит мониторинг отклоненных заявок, в части соблюдения должностной инструкции верификатора и выявления мошеннических действии со стороны потенциальных заемщиков, с целью модернизации (улучшения) технологических процессов МФО.

ГЛАВА 4. БЕЗОПАСНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ И ИНЫХ ДОКУМЕНТОВ

11. В целях обеспечения информационной безопасности МФО выполняются следующие условия:

- по организации системы управления информационной безопасностью;
- по организации доступа к информационным активам;
- по обеспечению безопасности информационной инфраструктуры;
- по осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
- по проведению анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;
- по обеспечению информационной безопасности при доступе третьих лиц к информационным активам;
- по проведению внутренних проверок состояния информационной безопасности;
- по процессам системы управления информационной безопасностью.

12. 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);

13. Требования к обеспечению информационной безопасности при организации деятельности МФО в части договоров на предоставление сведений о потенциальных заемщиках (данные об официальных доходах, перечислениях из ГФСС, о количестве и средней сумме пенсионных выплат из республиканского бюджета, данных кредитного отчета и другие отчеты) от ТОО «Первое кредитное бюро» (далее – ПКБ) в рамках заключенных договоров:

13.1. МФО обеспечивает конфиденциальность и целостность информации, получаемой из информационной системы ПКБ.

13.2. МФО обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями Договоров, заключенных с ПКБ.

13.3. МФО обеспечивает исполнение организационно-технических, технологических требований и мер, необходимых для функционирования и защиты системного и прикладного программного обеспечения, используемого для взаимодействия с информационной системой ПКБ и обработки получаемой из нее информации.

13.4. При использовании оборудования для работы с информационной системой ПКБ учитывается необходимость его защиты от несанкционированного доступа, а также защиты носителей информации и сетевых ресурсов, используемых для работы с информационной системой ПКБ.

13.5. МФО определяет и утверждает перечень ответственных лиц.

13.6. МФО обеспечивает наличие подписанных ответственными (ответственным) лицами (лицом) организации обязательств о неразглашении и нераспространении информации, ставшей им известной в процессе исполнения ими функциональных обязанностей.

13.7. МФО обеспечивает наличие внутренних документов, определяющих порядок определения и утверждения перечня ответственных лиц, их права и ответственность (включая должностные инструкции).

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

13.9. Учетная запись ответственного лица, по которой он идентифицируется в информационной системе ПКБ, соответствует конкретному физическому лицу.

13.10. МФО по запросу уполномоченного органа представляет сведения, подтверждающие его соответствие требованиям, предусмотренным в договорах с ПКБ.

13.11. Операционная система рабочей станции обеспечивает функции идентификации и аутентификации пользователя, а также разграничения прав доступа пользователей и авторизации в соответствии с назначенными правами.

13.12. МФО использует собственную рабочую станцию.

13.13. При использовании рабочей станции для подключения к информационной системе Кредитного бюро одновременное подключение к другим ресурсам сети интернет не производится.

13.14. Работники МФО обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.

13.15. Работники МФО обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы Кредитного бюро.

14. Ответственность за обеспечение информационной безопасности МФО возлагается на все структурные подразделения МФО в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами (в случае наличия).

15. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами МФО и законодательством РК. Все работники МФО несут персональную ответственность за нарушение и/или невыполнение установленных требований и мероприятий по защите информации и средств ее обработки, и обязаны сообщать обо всех выявленных нарушениях и инцидентах в ответственное за обеспечение безопасности подразделение. Должностные инструкции всех работников МФО должны содержать требования по обеспечению и соблюдению информационной безопасности.

ГЛАВА 5. МЕРЫ ПРОФИЛАКТИКИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

16. В профилактике инцидентов кибербезопасности важную роль играет соблюдение соответствующих национальных и международных требований при разработке программного обеспечения, проектировании компонентов информационных систем и инфраструктуры финансового сектора. МФО выполняет регулярную оценку рисков кибербезопасности, которая служит основой для выработки и применения мер по минимизации данных рисков, а также оценки эффективности реализованных мер.

17. Учитываются результаты, полученные на этапе профилактики (предотвращения), а также опыт уже обработанных инцидентов. Своевременно оценивается характер, масштабы и последствия инцидентов кибербезопасности, в целях снижения результатов их воздействия, своевременноуведомляются внутренние и внешние заинтересованные стороны и координируются совместные действия по реагированию. К заинтересованным сторонам относятся:

- Национальный Банк Республики Казахстан;
- Иные уполномоченные государственные и законодательные органы, осуществляющие регулирование деятельности МФО;
- заемщики;
- кредиторы и инвесторы;
- работники структурных подразделений, осуществляющие взаимодействие в процессе осуществления деятельности МФО;
- поставщики услуг.

18. Обеспечивается продолжение операционной деятельности после инцидента при

одновременном выполнении процедур восстановления, в том числе:

- устранения последствий инцидента;
- восстановления нормального состояния информационных систем и данных с подтверждением их нормального состояния;
- выявления и устранения уязвимостей, которые были использованы в рамках инцидента, в целях недопущения подобных инцидентов в будущем;

19. Повышение информированности и компетенции, как пользователей, так и работников (повышение квалификации, обучение) помогут устранить риски и создать культуру безопасного создания и использования информации в МФО. На этапе повышения осведомленности следует использовать опыт, полученный в ходе профилактики и реагирования, чтобы пользователи были ознакомлены с реальными рисками и эффективными методами их минимизации.

20. В случае обнаружения несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, ее несанкционированного изменения, осуществления несанкционированных действий со стороны третьих лиц, МФО незамедлительно принимает меры для устранения причин и последствий таких действий, а также в течение одного рабочего дня информирует об этом уполномоченный орган.

21. МФО принимает меры по предотвращению использования действующих или внедряемых способов и технологий предоставления микрокредитов электронным способом в схемах легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма. При предоставлении микрокредитов и проведении кредитного скорринга потенциального заемщика МФО применяет необходимые меры, предусмотренные Законом Республики Казахстан от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон о ПОДФТ), а также в соответствии с Постановлением Правления Национального Банка Республики Казахстан О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 25 декабря 2013 года № 292 "О введении ограничений на проведение отдельных видов банковских и других операций финансовыми организациями".

Глава 6. КОНФИДЕНЦИАЛЬНОСТЬ

22. Главным требованием конфиденциальности является обеспечение предоставления информации только авторизированным лицам.

23. При работе с ИС должна исключаться возможность наблюдения за отображаемой информацией посторонними лицами.

24. В ИС не должны размещаться документы, содержащие государственные секреты, коммерческую тайну и иную информацию с ограниченным доступом.

25. Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные в установленном порядке носители информации.

26. При работе с ИС должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.

Глава 7. СОГЛАШЕНИЯ О КОНФИДЕНЦИАЛЬНОСТИ

27. Требования по соглашениям о конфиденциальности или неразглашении, отражающие потребности по защите безопасности, должны быть определены и регулярно пересмотрены.

28. Для определения требований по соглашениям о конфиденциальности или неразглашении необходимо рассмотреть следующие элементы:

- определение информации, которая должна быть защищена (т.е. конфиденциальная информация или информация, содержащая коммерческую тайну);
- предполагаемая продолжительности соглашения, включая случаи, когда конфиденциальность должна поддерживаться бесконечно;
- требуемые действия по окончанию соглашения;
- обязанности и действия подписавших сторон во избежание несанкционированного разглашения информации (такого как «принцип необходимого знания»);
- собственность на информацию, коммерческие секреты и интеллектуальную собственность и то, как она связана с защитой конфиденциальной информации;
- разрешённое использование конфиденциальной информации и право подписавшей стороны использовать информацию;
- право аудита и мониторинга действий, в которых задействована конфиденциальная информация;
- процесс уведомления и сообщения о несанкционированном разглашении или нарушении конфиденциальности информации и коммерческой тайны;
- условия о возврате или уничтожении информации при прекращении действия соглашения;
- предполагаемые действия в случае нарушения данного соглашения.

В соглашении о конфиденциальности или неразглашении могут потребоваться другие элементы, основанные на требованиях безопасности. Соглашения о конфиденциальности и неразглашении должны соответствовать всем применяемым правовым нормам и правилам юрисдикции, которые применяются.

Глава 8. ТРЕБОВАНИЯ

8.1. Требования к обучению и осведомленности в вопросах ИБ

29. Работники МФО должны быть ознакомлены с политикой ИБ.
30. Работники МФО, обеспечивающие функционирование ИС должны проходить регулярно инструктаж по соблюдению ИБ.
31. Работники МФО обязаны как можно быстрее сообщать о любых событиях в сфере ИБ ответственным за ИБ лицам.

8.2. Требования по бесперебойному питанию

32. Бесперебойное электропитание обеспечивается ИБП (источником бесперебойного питания) необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и сворачивание операционной системы при отключении внешнего электропитания.

ГЛАВА 9. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В НАСТОЯЩУЮ ПОЛИТИКУ

33. Предложения о внесении изменений и дополнений в настоящую Политику могут быть инициированы любым сотрудником МФО посредством предоставления их в письменном виде уполномоченному лицу МФО.
34. Внесение изменений и дополнений в настоящую Политику производятся в соответствии с изменениями в Законодательстве Республики Казахстан и при необходимости.