УТВЕРЖДЕНА
Протоколом внеочередного общего собрания участников
ТОО Микрофинансовая организация «Сенат 2050»
№ 4 от «02» мая 2021 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ ПОСРЕДСТВОМ ИНТЕРНЕТ РЕСУРСА ТОО «Микрофинансовая организация «Сенат 2050»

г. Караганда

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика информационной безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет ресурса ТОО «Микрофинансовая организация «Сенат 2050» (далее – Политика) разработана в соответствии с нормами действующего законодательства Республики Казахстан в сфере информационной безопасности; Законом Республики Казахстан «О микрофинансовой деятельности»; Правилами предоставления микрокредитов электронным способом, утвержденными постановлением Правления Национального Банка Республики Казахстан от 28 ноября 2019 года № 217; Нормативно-правовыми актами Республики Казахстан, а также внутренними документами ТОО «Микрофинансовая организация «Сенат 2050» (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 необходима 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;
- **приоритетность** – категорирование (ранжирование) всех информационных ресурсов МФО по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности.

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 замышляемых правонарушений со стороны третьих лиц.

5. Настоящая Политика обязательна для исполнения всеми работниками МФО, стажерами, практикантами, а также должна доводиться до сведения заемщиков и иных третьих лиц, имеющих доступ к информационным системам и документам МФО, 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.

ГЛАВА 2. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7. Основными мерами по обеспечению информационной безопасности МФО являются:

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

7.1. 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;
- отслеживание и улучшение морально-делового климата в коллективе;
- определение действий при возникновении чрезвычайных ситуаций;
- проведение профилактических мер при приеме на работу и увольнении работников МФО.

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

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

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

- использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
- использование средств защиты периметра (firewall, IPS и т.п.);
- применение комплексной антивирусной защиты;
- использование средств информационной безопасности, встроенных в информационные системы;
- 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.

ГЛАВА 3. БИЗНЕС ПРОЦЕСС МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ПОСРЕДСТВОМ ДОСТУПА НА САЙТ МФО

8. Заемщик, выразивший намерение получить микрокредит электронным способом:

- входит в свой личный кабинет с использованием средств идентификации, или/
- указывает тип займа (Общий / Госслужащий / Пенсионер / Многодетная мать / Люди с ограниченными возможностями) и обеспечивает заполнение следующей необходимой информации: фамилия, имя, отчество; пол; дата рождения; гражданство; ИИН; адрес электронной почты (Email); отметить галочку (да/нет) в графе сведения о работе; общий доход; данные удостоверения личности; загружает фотографию Заемщика (в анфас на светлом фоне, с нейтральным выражением лица и закрытым ртом); загрузить любой документ, подтверждающий статус Заемщика; фамилия, имя, отчество, номер телефона поручителя; отметить галочку степень отношений с поручителем; абонентский номер сотовой связи; вводит уникальный код отправленный на абонентский номер сотовой связи Заемщика в виде короткого текстового сообщения (SMS).
- При заполнении анкеты Заемщик по собственному желанию выбирает способ получения микрокредита, заполняя необходимые поля (Переводом на карту / Переводом на карту (по номеру IBAN) / На расчетный счет в банке (по номеру IBAN) / Наличными в отделении МФО или КазПочта); (номер банковского счета и наименование банка; данные банковской карты).

9. Заемщик подтверждает подлинность заполненных контактных данных и отправляет заявление, согласие, договор посредством активации в личном кабинете заемщика на сайте уникального кода (простая электронная подпись), направленного МФО на мобильный телефон, указанный им при заполнении анкеты (регистрации) на сайте.

10. Регистрация Заемщика в личном кабинете осуществляется способом идентификации и аутентификации Заемщика в личном кабинете: 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); использования программного обеспечения, соответствующего следующим требованиям: обеспечение проверки и подтверждения изображения клиента в режиме реального времени с его изображением на документе, удостоверяющем личность обеспечение безопасности персональных данных клиента при обмене и хранении информации; защита от использования распечатанного бумажного изображения лица клиента; защита от возможности дублирования воспроизведения видео или фотоизображения с другого периферийного устройства.

11. Доступ заемщику в личный кабинет предоставляется после его идентификации и аутентификации. Уникальный идентификатор, установленный МФО, в комбинации с установленным заемщиком или динамически сгенерированным паролем, представляющие собой комбинацию букв, цифр или символов. Способы идентификации и аутентификации определяются внутренними процедурами безопасности и защиты информации от несанкционированного доступа МФО.

12. Личный кабинет предоставляет заемщику возможность осуществлять следующие, но, не ограничиваясь ими, действия:

- подача заявления на получение микрокредита;
- просмотр текущих микрокредитов;
- просмотр информации (истории) полученных микрозаймов;
- смена пароля.

ГЛАВА 4. БЕЗОПАСНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ И ИНЫХ ДОКУМЕНТОВ

13. 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 средствам криптографической защиты информации;
- по обеспечению информационной безопасности при доступе третьих лиц к информационным активам;
- по проведению внутренних проверок состояния информационной безопасности;
- по процессам системы управления информационной безопасностью.

14. 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, телефаксу, телексу и т.п. в виде электрических сигналов;
- присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

15. 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:

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

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

15.3. 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.

15.4. 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.

15.5. МФО определяет и утверждает перечень ответственных лиц.

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

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

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

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

15.10. МФО проводит плановые и внеплановые проверки соответствия рабочих станций (терминалов, мобильных приложений, сайта) Политике информационной безопасности.

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

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

15.13. МФО использует собственную рабочую станцию.

15.14. При использовании рабочей станции для подключения к информационной системе Кредитного бюро одновременное подключение к другим ресурсам сети интернет не производится.
15.15. Работники МФО обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к информационным системам.
15.16. Работники МФО обеспечивают конфиденциальность информации, ставшей им известной в процессе использования информационной системы Кредитного бюро.
16. 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.
17. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами МФО и законодательством РК.

ГЛАВА 5. МЕРЫ ПРОФИЛАКТИКИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

18. 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.
19. 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, своевременно уведомляются 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.

20. 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;
- обеспечения надлежащего информационного обмена внутри страны и за ее пределами.

21. 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.
22. 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.

23. 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 скоринга 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. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В НАСТОЯЩУЮ ПОЛИТИКУ

24. Предложения о внесении изменений и дополнений в настоящую Политику могут быть инициированы любым сотрудником МФО посредством предоставления их в письменном виде директору МФО.

25. Внесение изменений и дополнений в настоящую Политику производятся в соответствии с изменениями в Законодательстве Республики Казахстан и при необходимости.