Версия № 3 от «28» сентября 2022 г.

«Утверждено»
Решением Единственного участника
ТОО «МФО «Взаймы»
от «28» сентября 2022 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОННИРОВАННОГО ДОСТУПА ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА, МОБИЛЬНОГО ПРИЛОЖЕНИЯ И (ИЛИ) ТЕРМИНАЛА В ТОО «МФО «ВЗАЙМЫ»

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса, мобильного приложения и (или) терминала в ТОО «МФО «Взаймы» (далее - Политика) разработана в соответствии с нормами действующего законодательства Республики Казахстан в сфере информационной безопасности, Актами уполномоченного органа и внутренними документами ТОО «МФО «Взаймы» (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 не является самоцелью, ее обеспечение 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;
   - 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, в том числе минимизация угроз информационной безопасности, т.е. совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;
- способы двухфакторной аутентификации и верификации потенциальных заемщиков посредством интернет-ресурса, мобильного приложения и (или) терминала;
- 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. Положения настоящей Политики распространяются на следующий перечень объектов:
- работники структурных подразделений МФО (в том числе стажеры, практиканты);
- заемщики МФО и иные третьи лица, имеющие доступ к информационным системам и документам МФО, в той их части, которая непосредственно взаимосвязана с МФО и их деятельностью;
- поставщики, третьи лица и стороны, имеющие договорные отношения с МФО;
- информационные ресурсы МФО, составляющие конфиденциальную информацию, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности, информационные ресурсы (базы данных, файлы, системная документация, руководства пользователя, учебные материалы, политики и процедуры и т.п.), в том числе общедоступная информация, представленная в электронном виде;

6. информационная инфраструктура МФО, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, носители информации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы IT ресурсов. Настоящая Политика является общедоступным документом и размещается на официальном Интернет-ресурсе МФО https://kreditomat.kz/.

7. 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

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;
- 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.

8.2.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 и третьих лиц 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 (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. ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9. Для оценки рисков информационной безопасности МФО проводятся следующие мероприятия:

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

10. В перечень критичных информационных активов включаются информационные активы, убытки от нарушения свойств которых превышают установленный уровень существенности убытков от нарушения информационной безопасности.

11. В целях осуществления оценки рисков информационной безопасности для критичных информационных активов МФО обеспечивает реализацию следующих процессов:

- идентификация угроз информационной безопасности критичным информационным активам;
- идентификация источников угроз информационной безопасности, релевантных для критичных информационных активов;
- идентификация уязвимостей критичных информационных активов;
- идентификация существующих мер управления рисками информационной безопасности;
- оценка вероятности реализации угроз информационной безопасности критичным информационным активам источниками угроз информационной безопасности;
- оценка уровня рисков информационной безопасности.

12. Идентификация угроз информационной безопасности критичным информационным активам осуществляется подразделением по информационной безопасности. Для каждого критичного информационного актива анализируются угрозы информационной безопасности.

13. Идентификация источников угроз информационной безопасности, релевантных для критичных информационных активов, осуществляется подразделением по информационной безопасности МФО с учетом источников угроз информационной безопасности.

14. Идентификация уязвимостей критичных информационных активов осуществляется подразделением по информационной безопасности МФО, с учетом следующей информации о (об):

- конструкции информационного актива;
- физическом расположении информационного актива;
- известных ошибках в программном коде;
- ошибках в конфигурации;
- недостатках процесса эксплуатации информационного актива.

15. Идентификация существующих мер управления рисками информационной безопасности для критичных информационных активов осуществляется подразделением по информационной безопасности, с учетом информации об организационных и технических мероприятиях, направленных на исправление существующих недостатков в процессе обеспечения информационной безопасности критичных информационных активов либо последствий ее нарушения.

16. Оценка вероятности реализации угроз информационной безопасности критичным информационным активам источниками угроз информационной безопасности осуществляется подразделением по информационной безопасности для всех релевантных для критичного информационного актива комбинаций источника угрозы информационной безопасности, угрозы информационной безопасности и уязвимости, с учетом следующей информации:

- данные о расположении источника угрозы информационной безопасности относительно соответствующих критичных информационных активов (внутренний или внешний). Для внутренних источников угроз информационной безопасности учитывается количество пользователей актива, для внешних источников угроз информационной безопасности - наличие возможного доступа извне периметра защиты;
- данные об уровне доступа источника угрозы информационной безопасности;
- статистические данные о частоте реализации угрозы информационной безопасности критичному информационному активу в прошлом;
- информация о сложности реализации угрозы информационной безопасности критичному информационному активу;
- данные о наличии у рассматриваемых критичных информационных активов защитных мер.

17. При привлечении к оценке вероятности реализации угрозы информационной безопасности критичным информационным активам источниками угроз информационной безопасности нескольких экспертов и получении разных оценок итоговая, обобщенная оценка принимается равной оценке, определяющей наибольшую вероятность.

18. Оценка уровня рисков информационной безопасности проводится на основании сопоставления оценок вероятности реализации угрозы информационной безопасности критичным информационным активам источниками угроз информационной безопасности и оценок соответствующих потенциальных убытков от нарушения конфиденциальности, целостности или доступности критичного информационного актива.

ГЛАВА 4. БИЗНЕС-ПРОЦЕСС ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ПОСРЕДСТВОМ ТЕРМИНАЛА/МОБИЛЬНОГО ПРИЛОЖЕНИЯ

19. Двухфакторная аутентификация и верификация посредством терминала/мобильного приложения включает в себя:

- Фактор владения (получение уникального кода смс-сообщением и ввод данного кода);
- Фактор неотъемлемости (сканирование документа личности, в трех цветовых диапазонах, онлайн фото, биометрия лица);

20. Бизнес-процесс двухфакторной аутентификации и верификации посредством терминалов/мобильного приложения осуществляется следующим образом:

20.1. Терминал/мобильное приложение запрашивает номер телефона потенциального заемщика, для отправки смс-сообщения с уникальным кодом, который действует в течение 1-ой минуты. Код в свою очередь вводится в терминал, тем самым активирует терминал/мобильное приложение к дальнейшей работе. Данное действие подтверждает, что заемщик имеет при себе данный номер и имеет полный доступ к нему, т.е. определяется фактор владения.

20.2. После активации, потенциальному заемщику необходимо сфотографироваться, поместить лицо в объектив фронтальной камеры и следовать инструкциям на экране, обязательно направив взгляд на камеру, при этом, необходимо снять очки и головной убор, снимок будет сделан автоматически. Если системе не удастся распознать вашу биометрию на фото, необходимо пройти процедуру повторно. После успешного выполнения описанных выше шагов в основной форме верификации появится сообщение о проверке документов. В момент получения фотографии производится видеосъемка лица потенциального заемщика и идет поиск изменении показателей мимики в биометрии лица и сравниваются общие биометрические особенности лица в видео с фотографией. Это служит доказательством того, что полученная фотография клиента сделана в терминале с образа живого, двигающегося человека.

20.3. Следующим действием осуществляется сканирование удостоверения личности. Документ (удостоверение личности) помещается на стекло сканера и сканируется или необходимо сфотографировать в мобильном приложении с двух сторон (лицевую и после обратную сторону).

20.4. После получения изображения документа (удостоверения личности) клиента, запрограммированная система осуществляет проверку его подлинности на соответствие всех степеней защиты в ультрафиолетовом и инфракрасном спектре, срок действия документа, а также водяные знаки, согласно требованиям законодательства Республики Казахстан. Распознавание ключевых данных, таких как ИИН гарантируется наличием проверочной цифры в зоне MRZ документа.

После получения вышеуказанной информации, осуществляется автоматическое сравнение биометрии лица с удостоверением личности, а также программное обеспечение осуществляет надлежащую проверку потенциального клиента в соответствии с законодательством РК в сфере МФО, противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и внутренними документами.

20.5. При первичном обращении потенциального клиента/заемщика либо наличия отклонения от запрограммированных степеней идентификации, система помечает данную заявку как сомнительную и направляет на дополнительную проверку в центр обмена идентификационными данными (далее по тексту-ЦОИД) или/и к верификаторам.

20.6. Сомнительная заявка отправляется в ЦОИД или/и к верификаторам для анализа. Результаты анализа предоставляются по истечению 1-2 минут, с момента поступления заявки. Анализируются следующие показатели, но не ограничиваясь:

- Срок действия документа, расхождение ИИН с датой рождения, изображения документа (удостоверение личности) в ультрафиолетовом спектре, определяя имеются ли водяные знаки и почему их плохо видно (грязь, потертость на документе и т.п.);
- биометрии лица (фото) потенциального заемщика, в случае если потенциальный заемщик сильно поправился, похудел или постарел;

- биометрии лица (фото) потенциального заемщика среди биометрии (фото) лиц других клиентов, т.е. потенциальный заемщик до текущей заявки уже обращался в МФО для получения кредита под другим документом (удостоверением личности).
- в случае если на онлай-фото также присутствует фото третьего лица, то верификатор совершает звонок по данной заявки, задает дополнительные вопросы, после которых определяет содержание волеизъявления потенциального заёмщика.

20.7. По итогам анализа ЦОИД и/или верификация могут принять отрицательное решение, т.е. анализируемые сведения ниже установленной доли в процентном выражении по степени соответствия предоставленным МФО биометрических персональных данных потенциального клиента биометрическим персональным данным, содержащимся в соответствующих источниках.

20.8. Кроме того, верификация потенциальному заемщику в момент предоставления отрицательного решения в оформлении микрокредита, в обязательном порядке отображают причину отказа из шаблонов. Верификатор имеет право внести потенциального клиента/Заемщика посредством программного обеспечения МФО в Реестр неплатежеспособных заемщиков с указанием причины, совпадающей с причиной отказа потенциальному клиенту/Заемщику. И в последующем при повторном обращении данного лица в МФО, система сразу же отображает на дисплее терминала отказ в оформлении микрокредита.

20.9. В случае, если ЦОИД и/или верификация принимают положительное решение по сомнительной заявке, потенциальному клиенту необходимо выбрать сумму и срок предоставления микрокредита.

20.10. Также в личном кабинете потенциальный заемщик выбирает способ получения денежных средств:

Терминал- путем перечисления на счет платежной карты или банковский счет или путем получения в Терминале МФО;

Мобильное приложение - путем получения в Терминале МФО, путем перечисления на счет платежной карты или банковский счет, путем получения в отделении АО «Казпочта», путем получения в кассе МФО.

20.11. Потенциальному клиенту отображается на дисплее терминала/мобильного приложения проект кредитного договора.

20.12. Клиенту необходимо внимательно ознакомиться с договором и в случае согласия, нажать на дисплее терминала/мобильном приложении: «Получить СМС-код» для подписания кредитного договора.

20.13. Далее, на номер клиента, который он использовал для активации, приходит смс-сообщение с уникальным 4-значным кодом. Данный СМС-код клиенту необходимо ввести в терминал/мобильное приложение, тем самым подписать микрокредитный договор.

ГЛАВА 5. БЕЗОПАСНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ И ИНЫХ ДОКУМЕНТОВ

12. 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.

13. 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.

14. 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 кредитного бюро(далее по тексту - КБ) в рамках заключенных договоров**:**

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

14.18. МФО обеспечивает надлежащий уровень информационной безопасности в соответствии с условиями Договоров, заключенных с КБ.

14.19. 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 КБ и обработки, получаемой из нее информации.

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

14.21. МФО определяет и утверждает перечень ответственных лиц.

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

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

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

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

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

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

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

14.29. МФО использует собственную рабочую станцию.

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

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

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

15. 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.

16. За нарушение требований настоящей Политики и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами МФО и законодательством РК.

ГЛАВА 6. МЕРЫ ПРОФИЛАКТИКИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

17. 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.

18. 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.

19. 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.

20. 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.

21. Классическая модель информационной безопасности базируется на обеспечении трех значимых для безопасности информации атрибутов: конфиденциальность, целостность и доступность.

22. Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем.

23. Если доступ к информации получает неуполномоченное лицо, происходят несанкционированный доступ или нарушение конфиденциальности.

24. Доступность (возможность за разумное время получить требуемую информационную услугу)

25. Целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

26. 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.

27. 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 7. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В НАСТОЯЩУЮ ПОЛИТИКУ

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

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