УТВЕРЖДАЮ
Директор
ТОО "Микрофинансовая организация аФинанс"

_____/ Бельдеубаев М.
Приказ № ____-О/Д от "01" января 2021 года

ПРОЦЕДУРЫ
безопасности и защиты информации от несанкционированного доступа при предоставлении услуг МФО посредством интернет-ресурса www.turbomoney.kz

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящие Процедуры безопасности и защиты информации от несанкционированного доступа при предоставлении услуг посредством интернет-ресурса в ТОО «Микрофинансовая организация аФинанс» (далее – Процедуры) разработаны в соответствии с нормами действующего законодательства Республики Казахстан в сфере информационной безопасности, актами уполномоченного органа и внутренними документами ТОО «Микрофинансовая организация аФинанс» (далее - МФО).

2. Основной целью Процедуры, 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 Процедуры 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. Настоящие Процедуры определяют:

- Основные меры по обеспечению информационной безопасности МФО;
- Бизнес процесс многофакторной аутентификации и верификации потенциальных заемщиков посредством интернет-ресурса;
- Программно-технические средства защиты информации от несанкционированного доступа при предоставлении услуг МФО посредством интернет-ресурса;
- Описание функционала и техническая характеристика Программного обеспечения по распознаванию удостоверяющих документов;
- 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. Настоящие Процедуры обязательны 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. 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 Процедуры;
- контроль соответствия бизнес-процессов требованиям Процедуры;
- 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 АУДЕНТИФИКАЦИИ И ВЕРИФИКАЦИИ ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА

8. Многофакторная аутентификация и верификация посредством интернет-ресурса www.turbomoney.kz включает в себя:

- Смс - сообщение;
- Система определения живости пользователя «VeriLive»;
- Система распознавания удостоверяющих документов «VeriDoc»;
- Система распознавания лиц «VeriFace».

9. Бизнес процесс многофакторной аутентификации и верификации интернет-ресурса www.turbomoney.kz осуществляется следующим образом:

9.1. На интернет-ресурсе www.turbomoney.kz потенциальный заемщик заполняет заявку на получение микрокредита, путем ввода ИИН, ФИО, а также номера мобильного телефона, для отправки смс-сообщения с уникальным кодом (далее – «Пароль»). Пароль в свою очередь вводится на вкладке «Регистрация» на интернет-ресурсе www.turbomoney.kz, тем самым активируя личный кабинет заемщика. Данное действие подтверждает, что заемщик имеет при себе данный номер и имеет полный доступ к нему.

9.2. После активации и получения доступа в личный кабинет на интернет-ресурсе www.turbomoney.kz, потенциальному заемщику необходимо сфотографироваться, обязательно направив взгляд на камеру мобильного телефона. При этом, необходимо снять очки и головной убор.

9.3. В момент получения фотографии производится видеосъемка лица и потенциального заемщика и идет поиск изменении показателей мимики в биометрии лица перед камерой и сравниваются общие биометрические особенности лица в видео с фотографией. Это служит доказательством того, что полученная фотография заемщика сделана через программное обеспечение "Система определения живости «**VeriLive**» с образа живого, двигающегося человека.

9.4. Следующим действием осуществляется сканирование удостоверения личности через программное обеспечение «**VeriDoc**». Документ (удостоверение личности) фотографируется через камеру мобильного телефона, после чего сканируется с двух

сторон.

9.5. После получения изображения документа (удостоверения личности) заемщика, программное обеспечение «**VeriFace**» осуществляет проверку его подлинности. Распознавание ключевых данных, таких как ИИН гарантируется наличием проверочной цифры в зоне MRZ документа.

9.6. Полученную информацию интернет-сайт www.turbomoney.kz отправляет в ТОО «Первое кредитное бюро» (далее - ПКБ) на предмет проверки потенциального заемщика по имеющейся базе данных.

9.7. В случае получения положительной информации от ПКБ, МФО принимает решение о выдаче микрокреита.

ГЛАВА 4. ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПРЕДОСТАВЛЕНИИ УСЛУГ МФО ПОСРЕДСТВОМ ИНТЕРНЕТ-РЕСУРСА

10. Программно-технические средства защиты информации от несанкционированного доступа при предоставлении услуг МФО посредством интернет-ресурса www.turbomoney.kz базируются на двух основных составляющих:
    1) организация топологии сети. На сервере, к которому открыт доступ из глобальной сети Интернет, конфиденциальная информация не хранится. Для этого сервер распределения ключей и база данных, содержащая информацию для обслуживания заемщиков, выносятся в отдельный сегмент сети, к которому невозможен доступ из глобальной сети;
    2) обеспечение безопасного обмена данными между заемщиком и сервером, доступным из глобальной сети. Для этого используются алгоритмы шифрования трафика, которые позволяют исключить ситуацию подмены сервера, раннее выявление недостатков в системе безопасности путем сопоставления протоколов обмена сообщениями на стороне заемщика и сервера. В случае обнаружения несовпадений транзакция отменяется, а ключ пользователя (или сервера) считается невалидным.
11. Конфиденциальность передаваемой информации обеспечивается шифрацией данных (SSL – англ. Secure Sockets Layer — протокол защищенных сокетов). Целостность передаваемой информации обеспечивается хешированием каждого SSL пакета.
12. Доступ к Интернет-ресурсу www.turbomoney.kz осуществляется посредством подключения к сайту www.turbomoney.kz по защищенному протоколу HTTPS.
13. Адрес в сети Интернет – www.turbomoney.kz принадлежит МФО. МФО гарантирует пользователям сервисов интернет-ресурса «wwww.turbomoney.kz» защиту их персональных и платежных данных.
14. Программно-технический комплекс интернет-ресурса www.turbomoney.kz выделен в отдельную защищенную подсеть.
15. Допуск заемщика в личный кабинет осуществляется после его идентификации и аутентификации. Для регистрации заемщика в личном кабинете требуется ИИН заемщика.
16. Идентификация и аутентификации заемщика осуществляется МФО путем проверки правильности указания заемщиком:

16.1.при регистрации заемщика – ИИН и номер мобильного телефона заемщика;

16.2.при входе в личный кабинет – логина и пароля.

17. Для обеспечения защиты от несанкционированного доступа к информации, составляющей тайну предоставления микрокредита, МФО применяет автоматическую проверку правильности указания заемщиком логина и пароля при входе в личный кабинет.
18. Логином в системе интернет - ресурса www.turbomoney.kz является номер мобильного телефона, который заемщик указывает при прохождении процедуры Регистрации.
19. Заемщик в процессе его идентификация и аутентификации: а) указывает номер мобильного телефона, являющегося Логином, б) вводит Пароль, содержащийся в SMS - сообщении, высланный МФО на данный номер.
20. Если компьютер или мобильный телефон после входа заемщиком в личный кабинет остается бездействующим более 10 (десять) минут, осуществляется автоматический выход из личного кабинета и завершение сессии.
21. В целях безопасности сохранение логина и пароля заемщика для упрощения процедуры входа в личный кабинет не предусматривается.
22. МФО вправе в одностороннем порядке осуществлять мероприятия в сторону улучшения для заемщика, касающиеся усиления процедур безопасности от мошеннических действия, разглашения конфиденциальной информации, или иных противоправных действий в рамках выявления и предотвращения потенциальных угроз и рисков информационной безопасности.
23. МФО обеспечивает безопасное хранение 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. Хранение электронных сообщений и иных документов осуществляется в том формате, в котором они были сформированы, отправлены заемщику или получены от него.
24. 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.

ГЛАВА 5. БЕЗОПАСНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ СООБЩЕНИЙ И ИНЫХ ДОКУМЕНТОВ

25. 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.

26. 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.
- 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:

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

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

26.3. 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.

26.4. 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.

26.5. МФО определяет и утверждает перечень ответственных лиц.

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

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

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

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

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

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

26.12. МФО использует собственную рабочую станцию.

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

26.14. Работники МФО обеспечивают конфиденциальность персональных идентификационных и аутентификационных данных, используемых для доступа к

информационным системам.

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

26.16. Ответственность за обеспечение информационной безопасности МФО возлагается на все структурные подразделения МФО в рамках их полномочий и в соответствии с положениями, установленными настоящими Процедурами и разработанными на ее основе документами.

27. За нарушение требований настоящих Процедур и документов, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами МФО и законодательством РК.

ГЛАВА 6. МЕРЫ ПРОФИЛАКТИКИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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 НАСТОЯЩИЕ ПРОЦЕДУРЫ

34. Предложения о внесении изменений и дополнений в настоящие Процедуры могут быть инициированы любым сотрудником МФО посредством предоставления их в письменном виде директору МФО.
35. Внесение изменений и дополнений в настоящие Процедуры производятся в соответствии с изменениями в Законодательстве Республики Казахстан и при необходимости.