Утверждена
Приказом Генерального директора
ТОО «МФО «CASHDRIVE.KZ»
№24-Н от 15.06.2026
с введением в действие с 12.07.26 года

Политика информационной безопасности
ТОО МФО «CASHDRIVE.KZ»

1. Общие положения

1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом системы управления информационной безопасности ТОО МФО «CASHDRIVE.KZ.» (далее – МФО), определяющим цели, задачи и область действия системы управления информационной безопасностью МФО (далее - СУИБ).
2. МФО обеспечивает создание и функционирование СУИБ, являющейся частью общей системы управления МФО, предназначенной для управления процессом обеспечения информационной безопасности.
3. СУИБ обеспечивает защиту информационных ресурсов МФО, допускающую минимальный уровень потенциального ущерба для бизнес-процессов МФО.
4. Настоящая Политика разработана в соответствии с:
1) Постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 20 апреля 2026 года № 81 «Об утверждении минимальных требований по обеспечению информационной безопасности на финансовом рынке»;
2) Цифровым кодексом Республики Казахстан (Кодекс РК от 9 января 2026 года № 255-VIII);
3) Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»;
4) Законом Республики Казахстан от 28 августа 2009 года № 191-IV «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
5) Постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 29 октября 2020 года № 105 «Об утверждении Требований к Правилам внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения для организаций, осуществляющих отдельные виды банковских операций... и организаций, осуществляющих микрофинансовую деятельность».

5. МФО разрабатывает и утверждает Политику обработки персональных данных в соответствии с требованиями Закона Республики Казахстан «О персональных данных и их защите», определяющую цели, порядок и условия обработки персональных данных, права субъектов персональных данных и меры по обеспечению их защиты, иными регуляторными требованиями.

2. Цели, задачи и основные принципы построения системы управления информационной безопасностью

6. Основные цели СУИБ:
1) обеспечение надлежащей защиты информации в зависимости от ее значения для МФО;
2) обеспечение конфиденциальности, целостности и доступности информации, защиты персональных данных;
3) предотвращение несанкционированного физического и электронного доступа, повреждения и вмешательства в информацию и в средства обработки информации МФО.
7. К задачам СУИБ относятся:

1) категорирование информационных ресурсов;
2) организация доступа к информационным ресурсам;
3) обеспечение безопасности информационной инфраструктуры;
4) осуществление мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз и уязвимостей, противодействию атакам и расследованию инцидентов информационной безопасности;
5) проведение анализа информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах;
6) определение порядка управления средствами криптографической защиты информации;
7) обеспечение информационной безопасности при доступе третьих лиц к информационным ресурсам;
8) проведение внутренних проверок состояния информационной безопасности.
8. Построение СУИБ и ее функционирование осуществляются в соответствии со следующими основными принципами:
1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на информационные ресурсы МФО;
2) ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности, любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий для ведения бизнеса;
3) комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
4) документированность – все требования и меры информационной безопасности, а также результаты деятельности по обеспечению информационной безопасности документально зафиксированы;
5) адаптивность – определение и применение методов и средств защиты информационных ресурсов в соответствии с их критичностью;
6) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем информационным ресурсам, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;
7) специализация – реализация мер и эксплуатация технологических решений по обеспечению информационной безопасности должны осуществляться профессионально подготовленными специалистами;
8) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;
9) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений МФО, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;
10) подтверждаемость – свидетельства, подтверждающие исполнение требований по информационной безопасности и эффективности СУИБ, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

3. Область действия системы управления информационной безопасностью

9. Областью действия СУИБ являются основные бизнес-процессы МФО, непосредственно ориентированные на предоставление услуг клиентам, представляющие ценность для клиентов и

обеспечивающих получение прибыли, определенных с процедурой, определяющей классификацию бизнес-процессов, такие как:
1) критичные информационные активы, необходимые для функционирования основных бизнес-процессов;
2) информационные активы, необходимые для работы МФО, независимо от формы и вида их представления;
3) элементы ИТ-инфраструктуры, включая информационные технологии, технические и программные средства формирования, обработки, передачи, хранения (в том числе архивирования) и использования информации, в том числе базы данных, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены защищаемые элементы ИТ-инфраструктуры МФО;
4) процессы, регламенты и процедуры обработки информации в МФО;
5) персональные данные субъектов персональных данных (заемщик/созаемщик, гарант, залогодатель, работники, поставщики МФО (их работники) и т.п.).

4. Требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах МФО и мониторинг информации и доступа к ней

10. МФО обеспечивает ознакомление нового работника с основными внутренними документами и требованиями к обеспечению информационной безопасности под подпись не позднее 5 (пяти) рабочих дней с момента приема на работу. Результат ознакомления фиксируется в Листе ознакомления, который приобщается к личному делу работника, а также в соответствующем журнале инструктажа, подтверждающем прохождение работником инструктажа по информационной безопасности.
11. Доступ к информации и информационным системам МФО предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.
12. В информационных системах МФО используются только персонализированные пользовательские учетные записи пользователей.
13. Предоставление доступа к критичным информационным системам МФО производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям.
14. Доступ лицам, не являющимся работниками МФО (далее - третьи лица) к информационным ресурсам МФО предоставляется на период и в объеме, необходимых для проведения работ на основании соответствующего соглашения о соблюдении требований к информационной безопасности, за исключением случаев, предусмотренных законодательством Республики Казахстан. В соглашениях о соблюдении требований к информационной безопасности, заключаемых с третьими лицами, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения информационной безопасности, а также сбоев в работе информационных систем и нарушения их безопасности, вызванных вмешательством третьих лиц.
15. Доступ к информационным системам МФО осуществляется путем идентификации и аутентификации пользователей информационных систем. Идентификация и аутентификация пользователей информационных систем МФО производится посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов многофакторной аутентификации.
16. Использование технологических учетных записей допускается в соответствии с перечнем таких учетных записей для каждой информационной системы с указанием лиц, персонально ответственных за их использование и актуальность.
17. МФО применяет все необходимые организационные и технические меры, обеспечивающие эффективность процесса управления доступом к информационным активам.
18. В цифровых системах МФО используется функция ведения аудиторского следа, которая отражает как минимум:
1) события установления соединений, идентификации, аутентификации и авторизации (успешные и неуспешные), включая IP-адрес источника соединения;

2) события модификации настроек безопасности;
3) события модификации групп пользователей и их полномочий;
4) события модификации учетных записей пользователей и их полномочий;
5) события, отражающие установку обновлений и (или) изменений;
6) события изменения параметров ведения аудиторского следа.
19. При хранении аудиторского следа обеспечивается контроль его неизменности. Срок хранения аудиторского следа составляет не менее 1 (одного) года.
20. В целях обеспечения контроля деятельности пользователей и клиентов ведется аудиторский след действий их учетных записей в цифровых системах МФО.
21. Идентификация и аутентификация пользователя или клиента осуществляется при помощи одного или нескольких факторов, включая знание, владение или неотъемлемость. Фактор знания основывается на информации, которую должен знать пользователь или клиент. Фактор владения основывается на владении пользователя или клиента определенным физическим устройством или криптографическим ключом. Фактор неотъемлемости основывается на уникальных биометрических особенностях пользователя или клиента.
22. Доступ пользователей и клиентов извне периметра защиты МФО к цифровым системам осуществляется с применением как минимум двух различных факторов аутентификации.
23. Доступ работника МФО к цифровым системам осуществляется в соответствии с внутренними документами МФО при наличии утвержденных документов МФО, подтверждающи необходимость такого доступа для исполнения обязанностей работника.
24. Доступ третьих лиц к цифровым системам осуществляется в соответствии с внутренними документами МФО при наличии действующего договора, предусматривающего необходимость такого доступа третьим лицам к цифровым системам МФО.
25. Идентификация и аутентификация клиента МФО осуществляется в соответствии с внутренними документами МФО на основании данных, полученных при регистрации клиента МФО.
26. Регистрация клиента в цифровых системах МФО осуществляется в соответствии с внутренними документами МФО после подтверждения личности клиента. Для дистанционного подтверждения личности при регистрации применяется комбинация как минимум из следующих проверок:
1) биометрическая проверка клиента по изображению лица с использованием государственной базы данных изображений или по биометрическим данным, полученным при личном присутствии клиента посредством специально предназначенных для этого устройств МФО;
2) проверка владения телефонным номером, зарегистрированным в государственной базе номеров мобильных телефонов граждан, либо проверка владения закрытым ключом сертификата электронной цифровой подписи, выпущенного аккредитованным удостоверяющим центром.
27. В целях последующей идентификации и аутентификации клиента в ходе регистрации допускается сбор следующих данных:
1) пароль, задаваемый клиентом;
2) вектор инициализации, серийный номер или иная информация, необходимая для подключения аппаратного или программного генератора одноразовых паролей (OTP-генератора);
3) уникальный идентификатор установки мобильного приложения на мобильное устройство, а также индивидуальные характеристики мобильного устройства;
4) сертификат электронной цифровой подписи, соответствующий закрытому ключу, хранимому на устройстве клиента;
5) дополнительный номер мобильного телефона, владение клиента которым подтверждено;
6) биометрические данные клиента, проверенные посредством государственной базы данных изображений или полученные посредством устройств МФО;
7) открытый криптографический ключ, соответствующий закрытому криптографическому ключу, хранимому на устройстве клиента.
28. Проверка владения мобильным телефонным номером осуществляется путем отправки на проверяемый мобильный телефонный номер сгенерированного непредсказуемого кода с последующим получением данного кода от владельца мобильного телефонного номера аутентифицирующей системой.

29. Проверка владения закрытым ключом сертификата электронной цифровой подписи осуществляется в соответствии с правилами аккредитованного удостоверяющего центра, выпустившего данный сертификат электронной цифровой подписи.

5. Технические требования к обеспечению информационной безопасности

30. МФО обеспечивает функционирование периметра защиты МФО.
31. Телекоммуникационные соединения, выходящие за пределы периметра защиты МФО, подлежат шифрованию.
32. Почтовые сервисы МФО, используемые в том числе для взаимодействия с государственными органами и гражданами Республики Казахстан, функционируют только на цифровой инфраструктуре, физически размещённой на территории Республики Казахстан (далее - казахстанские адреса электронной почты).
33. МФО публикует в общедоступных источниках информацию о своих казахстанских адресах электронной почты с пояснением, что они должны использоваться гражданами Республики Казахстан для взаимодействия с МФО.
34. МФО использует почтовые сервисы, обеспечивающие при отправке и получении электронных почтовых сообщений применение следующих защитных механизмов электронной почты: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication Reporting & Conformance (DMARC).
35. МФО обеспечивает контроль изменения настроек и целостности конфигурационных файлов программно-аппаратных средств периметра защиты.
36. Работникам МФО не предоставляются права доступа локального администратора или аналогичные права доступа, за исключением случаев, когда права доступа локального администратора или права, аналогичные правам доступа локального администратора, требуются для функционирования программного обеспечения, используемого работником для исполнения своих функциональных обязанностей.
37. МФО использует антивирусные системы или системы, контролирующие целостность и неизменность программной среды, как на серверах, так и на рабочих станциях, ноутбуках, мобильных устройствах (при наличии технической возможности) МФО. При этом обеспечивается:
1) наличие лицензий, обновлений и технической поддержки;
2) обеспечение невозможности для конечного пользователя прерывания функционирования данной системы.
38. В случаях размещения МФО серверных мощностей в сторонних центрах обработки данных, использования внешних сервисов обработки и (или) хранения данных исключается возможность доступа третьих лиц к информации, передача которой третьим лицам не допускается в соответствии с гражданским, банковским законодательством Республики Казахстан, законодательством Республики Казахстан о персональных данных и их защите.
39. Резервное копирование цифровых систем и обрабатываемых в них данных обеспечивается МФО исходя из потребностей в восстановлении после сбоев в работе цифровых систем. Порядок и периодичность резервного копирования, хранения, восстановления данных, периодичность тестирования восстановления работоспособности цифровых систем из резервных копий определяется МФО во внутренних документах на основе проведенного анализа воздействия на бизнес.
40. МФО обеспечивает контроль изменения настроек и целостности конфигурационных файлов программно-аппаратных средств периметра защиты.

6. Требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности

41. МФО обеспечивает выделение ответственных работников по реагированию на инциденты информационной безопасности, в том числе по оповещению уполномоченного органа об

инцидентах информационной безопасности, связанных с незаконным доступом к персональным данным ограниченного доступа.

42. В целях обеспечения надлежащего мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности МФО обеспечивает:

1) внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс реагирования на инциденты информационной безопасности;

2) определение перечня событий информационной безопасности, подлежащих мониторингу, источников таких событий, периодичности, порядка и методов мониторинга событий информационной безопасности;

3) определение порядка отнесения событий информационной безопасности к инцидентам информационной безопасности, их классификации и приоритетности;

4) разработку, поддержание в актуальном состоянии стандартных процедур реагирования и обучение работников на инциденты информационной безопасности по вопросам применения стандартных процедур реагирования;

5) определение ответственных работников МФО, вовлеченных в процесс реагирования на инциденты информационной безопасности;

6) определение порядка принятия неотложных мер по устранению инцидентов информационной безопасности, установления причин возникновения инцидентов информационной безопасности и их последствий;

7) наделение ответственных работников полномочиямипо введению дополнительных мер контроля по частичной или полной остановке бизнес-процессов в случае выявления инцидента информационной безопасности;

8) определение порядка информирования руководящих работников МФО, подразделений МФО и уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций, в том числе для принятия решения о проведении внутреннего расследования инцидента информационной безопасности;

9) сбор и анализ материалов, необходимых для проведения внутреннего расследования инцидента информационной безопасности;

10) установление причин возникновения инцидента информационной безопасности и порядка реализации инцидента информационной безопасности;

11) оценка масштаба воздействия и ущерба от реализации инцидента информационной безопасности;

12) анализ эффективности принятых мер реагирования на расследуемый инцидент информационной безопасности;

13) подготовка заключения о результатах расследования инцидента информационной безопасности, в котором отражается информация об инциденте информационной безопасности, а также рекомендации по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторной реализации инцидента информационной безопасности.

43. МФО предоставляет в уполномоченный орган информацию о следующих выявленных инцидентах информационной безопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении;

2) несанкционированный доступ в цифровую систему;

3) атака «отказ в обслуживании» на цифровую систему или сеть передачи данных;

4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода денежных средств вследствие нарушения контролей информационной безопасности;

6) нарушение работы систем идентификации и аутентификации клиента;

7) иных инцидентах информационной безопасности, повлекших простои цифровых систем более одного часа.

Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется МФО незамедлительно посредством автоматизированной системы

уполномоченного органа, предназначенной для обработки информации о событиях и инцидентах информационной безопасности (далее - АСОИ) или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.
В случае недоступности вышеуказанных систем передача информации об инциденте осуществляется с телефонного номера МФО, указанного при регистрации МФО в АСОИ, на телефонный номер уполномоченного органа, указанный для связи на интернет-ресурсе уполномоченного органа в разделе «Информационная безопасность» с дублированием на бумажном носителе официальным письмом МФО.
При отсутствии подключения МФО к АСОИ информация об инцидентах информационной безопасности передаётся на адрес электронной почты Агентства, указанный на интернет-ресурсе уполномоченного органа в разделе «Информационная безопасность».

7. Требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности

44. МФО обеспечивает наличие документов, сведений и фактов, подтверждающих реализацию порядка реагирования на инциденты информационной безопасности, а также консолидацию, систематизацию, целостность и сохранность информации об инцидентах информационной безопасности, результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования на бумажном носителе и (или) в электронном виде.
45. Срок хранения информации об инцидентах информационной безопасности, результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования составляет не менее 5 (пяти) лет.
46. В целях повышения эффективности процесса мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности, не реже одного раза в год МФО обеспечивает:
1) проведение анализа выявленных инцидентов информационной безопасности и нанесенного ими ущерба для рассмотрения уполномоченными лицами МФО, с целью оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности, изменения бизнес процессов;
2) оценку эффективности с целью корректировки процесса реагирования на инциденты информационной безопасности с использованием метрик процесса реагирования на инциденты информационной безопасности;
3) пересмотр метрик процесса реагирования на инциденты информационной безопасности сучетом результата оценки эффективности процесса реагирования на инциденты информационной безопасности;
4) пересмотр перечня событий информационной безопасности, подлежащих мониторингу, источников событий, периодичности, порядка и методов мониторинга событий информационной безопасности.

8. Ответственность работников МФО за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей

47. Участниками СУИБ МФО являются:
1) единоличный исполнительный орган (генеральный директор);
2) подразделение по обеспечению информационной безопасности;
3) подразделение по информационным технологиям;
4) подразделение по управлению персоналом или работник, осуществляющий подбор кадров;
5) юридическое подразделение;
6) подразделение/работник по комплаенс-контролю;
7) подразделение внутреннего аудита;

8) подразделение/работник по управлению рисками информационной безопасности (риск-менеджер)

В случае отсутствия одного из подразделений в МФО их функции исполняют ответственные работники в силу возложенных на них задач согласно должностной инструкции или распорядительному акту.

48. Единоличный коллегиальный орган (далее - УО) МФО утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией. Подразделение по обеспечению информационной безопасности совместно с риск-менеджером в целях обеспечения конфиденциальности, целостности и доступности информации МФО осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений МФО по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности МФО, осуществляет контроль за ее актуальностью, вносит предложения единоличному исполнительному органу или иному коллегиальному органу/лицу, ответственному за обеспечение информационной безопасности МФО, по ее изменению/дополнению или несоответствию настоящей Политики законодательству Республики Казахстан целям, задачам, бизнес-процессам МФО и (или) иным внутренним нормативным документам (далее – ВНД) МФО, или несоответствию иных ВНД настоящей Политике;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности МФО;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности МФО, в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) подготавливает предложения для принятия УО решения по вопросам информационной безопасности;

8) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности МФО, а также предоставление доступа к ним;

9) определяет ограничения по использованию привилегированных учетных записей;

10) участвует в организации процесса повышения осведомленности работников МФО в области информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью МФО;

12) осуществляет информирование руководства МФО о состоянии системы управления информационной безопасностью МФО;

13) проводит оценку рисков информационной безопасности;

14) подготавливает и предоставляет отчетность о реализации существенных рисков информационной безопасности единоличному исполнительному органу или иному коллегиальному органу/лицу, ответственному за обеспечение информационной безопасности МФО, а также об устранении их последствий;

15) разрабатывает план мероприятий по реализации стратегии МФО в части обеспечения информационной безопасности, который раскрывает, но, не ограничиваясь, следующее:

– определение потребностей в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками информационной безопасности;

– описание требуемых мероприятий в области информационной безопасности с указанием сроков

и ответственных исполнителей за их реализацию.
Единоличный исполнительный орган МФО при формировании бюджета учитывает потребности в ресурсах для обеспечения информационной безопасности МФО.
49. Подразделение по информационным технологиям осуществляет следующие функции:
1) разрабатывает схемы информационной инфраструктуры МФО;
2) обеспечивает предоставление доступа пользователям к информационным активам МФО, за исключением специализированных информационных активов, доступ к которым предоставляется ИТ-менеджерами информационных систем;
3) обеспечивает конфигурирование системного и прикладного программного обеспечения МФО;
4) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем МФО (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с внутренними документами МФО;
5) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.
50. Подразделение/лицо по управлению персоналом осуществляет следующие функции:
1) обеспечивает подписание работниками МФО, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;
2) организует и проводит мероприятия по обеспечению осведомленности работников МФО в вопросах информационной безопасности.
51. Юридическое подразделение осуществляет правовую экспертизу внутренних нормативных документов МФО и соглашений (договоров) по вопросам обеспечения информационной безопасности.
52. Комплаенс-контролер совместно с юридическим подразделением определяет виды информации,подлежащие включению в перечень защищаемой информации.
53. Подразделение/работник по внутреннему аудиту (ревизор) проводит оценку состояния системы управления информационной безопасностью МФО в соответствии с внутренними нормативными документами МФО, регулирующими организацию системы внутреннего аудита МФО.
54. Подразделение/лицо по управлению рисками информационной безопасности (риск- менеджер) осуществляет функции, предусмотренные ВНД или нормативных правовых актов Республики Казахстан, регулирующих правила формирования системы управления рисками и внутреннего контроля для финансовых институтов.
55. Бизнес-владельцы информационных систем или подсистем:
1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг;
2) формируют и поддерживают актуальность матриц доступа к информационным системам.
56. Руководители структурных подразделений МФО:
1) обеспечивают ознакомление работников с ВНД, содержащими требования к информационной безопасности;
2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.
57. Работники структурных подразделений МФО:
1) отвечают за соблюдение требований к информационной безопасности, принятых в МФО;
2) контролируют исполнение требований к информационной безопасности третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;
3) извещают своего непосредственного руководителя и подразделение по обеспечению безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.
58. Первый руководитель МФО несет персональную ответственность за обеспечение информационной безопасности МФО.

59. Несоблюдение порядка и правил использования информационных ресурсов и принятых в МФО мер обеспечения информационной безопасности, при исполнении работником возложенных нанего функциональных обязанностей, влечет за собой ответственность в соответствии с законодательством Республики Казахстан, настоящей Политикой и иными ВНД.

9. Заключительные положения

60. Все вопросы, не урегулированные настоящей Политикой, решаются в соответствии с законодательством Республики Казахстан, ВНД и решениями единоличного исполнительного органа, коллегиального органа, а также сложившейся практикой деятельности МФО.
61. Настоящая Политика вступает в силу с даты утверждения ее утверждения и прекращает свое действие с момента признания ее утратившей силу.
62. Если в результате изменения законодательства Республики Казахстан отдельные нормы настоящей Политики вступают в противоречие с законодательством Республики Казахстан, то до момента внесения изменений в настоящую Политику необходимо руководствоваться законодательством Республики Казахстан и настоящей Политикой в части, не противоречащей законодательству Республики Казахстан.
63. Пересмотр настоящей Политики осуществляется ответственным работником по обеспечению безопасности не реже одного раза в год, а также при изменении законодательства Республики Казахстан, выявлении существенных недостатков, изменении организационной структуры или бизнес-процессов МФО.
64. Внеплановый пересмотр настоящей Политики осуществляется в случае:
1) изменения нормативных правовых документов Республики Казахстан, ВНД, определяющих требования к информационной безопасности;
2) выявления снижения общего уровня информационной безопасности МФО (по результатам внутреннего или внешнего аудита);
3) существенных изменений организационной и/или инфраструктуры, ресурсов и бизнес-процессов МФО;
4) выявления существенных недостатков при выполнении мероприятий, регламентированных настоящей Политикой, а также противоречий ее положений с другими ВНД.