Политика
информационной безопасности АО «KMF Банк»

Бизнес - владелец:	Департамент безопасности
Утверждена:	Протокол Совета Директоров от 12.11.2025 г. №3(9)
Введено в действие:	с 12.11.2025 г.
Признана утратившим силу:	Политика информационной безопасности АО «KMF Банк» утвержденная Протоколом Советом Директоров АО «МФО (KMF)» №6 от 15.07.2026
Уровень доступа к ВНД:	Неограниченный доступ

г. Алматы,
2025 г.

Оглавление

Глава 1. Общие положения 3
Глава 2. Информационная безопасность 4
Глава 3. Организация системы управления информационной безопасностью 5
§1.Определение системы управления информационной безопасностью 5
§2.Цели системы управления информационной безопасностью 5
§3.Задачи системы управления информационной безопасностью 5
§4.Принципы построения системы управления информационной безопасностью 6
§5.Область действия системы управления информационной безопасностью 6
§6.Реализация системы управления информационной безопасностью 7
§7.Направления развития и улучшения системы управления информационной безопасностью 8
§8.Требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах Банка 9
§9.Требования к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности 10
§10.Требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности 12
§11.Требования к проведению анализа информации об инцидентах информационной безопасности 13
Глава 4. Заключительные положения 14

Глава 1. Общие положения

1. Настоящая Политика информационной безопасности АО «KMF Банк» (далее – Политика) является внутренним нормативным документом и основой системы управления информационной безопасностью АО «KMF Банк» (далее – Банк).
2. Настоящая Политика разработана в соответствии с законодательством Республики Казахстан, в том числе Требованиями к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций, осуществляющих отдельные виды банковских операций, утвержденными постановлением Правления Национального Банка Республики Казахстан от 27 марта 2018 года № 48, серией международных стандартов по информационной безопасности ISO/IEC 27000 и внутренними нормативными документами Банка;
3. Целью настоящей Политики является декларирование официальной позиции Банка, утвержденной его руководством, в области обеспечения информационной безопасности, а также определение целей, задач, принципов построения и направлений развития системы управления информационной безопасностью.
4. Правление Банка инициирует, поддерживает, анализирует и контролирует выполнение процессов системы управления информационной безопасностью, способствующих созданию условий для устойчивого развития бизнеса с допустимым уровнем рисков информационной безопасности, формированию конкурентных преимуществ, обеспечению финансовой стабильности, рентабельности и повышению рейтинга Банка.
5. Совет Директоров Банка осуществляет стратегическое руководство в области информационной безопасности, обеспечивая интеграцию вопросов информационной безопасности в стратегию и операционную деятельность Банка. При формировании бюджета Совет Директоров учитывает потребности в ресурсах для обеспечения информационной безопасности с учетом стратегических целей Банка, требований законодательства и регулирующих органов, текущей и прогнозируемой среды угроз, а также обязательств перед заинтересованными сторонами.
6. Требования информационной безопасности, устанавливаемые настоящей Политикой, согласованы со стратегией развития Банка, интегрированы в его бизнес-процессы и направлены на минимизацию рисков информационной безопасности. Риски информационной безопасности рассматриваются как часть операционных рисков Банка и оказывают существенное влияние на его финансовую устойчивость и стабильность функционирования.
7. Требования настоящей Политики распространяются на все процессы, ресурсы и субъектов входящие в область действия системы управления информационной безопасностью, установленную настоящей Политикой.
8. Настоящая Политика является общедоступным документом и размещается на корпоративном сайте Банка, чтобы быть доступной для всех заинтересованных сторон.
9. В настоящей Политике используются следующие термины и определения:
    1) доступ - возможность использования информационных активов Банка;

2) инцидент информационной безопасности - отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;
3) информационный актив - совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;
4) информационно-коммуникационная инфраструктура (далее - информационная инфраструктура) - совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;
5) риск информационной безопасности - вероятное возникновение ущерба вследствие нарушения конфиденциальности, преднамеренного нарушения целостности или доступности информационных активов Банка.

Глава 2. Информационная безопасность

10. Под информационной безопасностью понимается состояние защищенности электронных информационных ресурсов, информационных систем и информационной инфраструктуры Банка от внешних и внутренних угроз, способных привести к материальному ущербу, нанести вред деловой репутации либо повлечь иной ущерб интересам Банка, его клиентов, работников, акционеров.
11. Под обеспечением информационной безопасности понимается процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов Банка.
12. В рамках обеспечения информационной безопасности поддерживаются главные атрибуты безопасности информации:
    1) конфиденциальность - свойство информации, при котором она не раскрывается и не становится доступной неавторизованным субъектам. Обеспечение конфиденциальности включает применение мер, направленных на предотвращение несанкционированного раскрытия информации;
    2) целостность - свойство информации, при котором сохраняется ее полнота, непротиворечивость и точность в процессе хранения, обработки и передачи. Обеспечение целостности включает применение мер, направленных на предотвращение и выявление несанкционированного создания, изменения или удаления информации;
    3) доступность - свойство информации быть доступной и пригодной к использованию по запросу уполномоченного субъекта. Обеспечение доступности включает применение мер, направленных на поддержание

доступа к информации, несмотря на возможные помехи, включая отказы систем и преднамеренные попытки нарушения доступности.

13. Основной целью деятельности по обеспечению информационной безопасности является защита информационных активов Банка, обеспечивающая минимальный уровень потенциального ущерба для бизнес-процессов Банка. Для достижения этой цели в Банке создается, функционирует и непрерывно улучшается система управления информационной безопасностью.

Глава 3. Организация системы управления информационной безопасностью

§1. Определение системы управления информационной безопасностью

14. Система управления информационной безопасностью представляет собой часть общей системы управления Банка, предназначенной для управления процессом обеспечения информационной безопасности.
15. Система управления информационной безопасностью обеспечивает системный, обоснованный и управляемый подход к принятию решений в области информационной безопасности посредством механизмов управления рисками.
16. Система управления информационной безопасностью включает в себя Политику, организационную структуру, процессы, ресурсы и документированную информацию, обеспечивающие эффективное управление информационной безопасностью.
17. Банк обеспечивает функционирование, надлежащий уровень зрелости, развитие и постоянное улучшение системы управления информационной безопасностью.

§2. Цели системы управления информационной безопасностью

18. Основные цели системы управления информационной безопасностью:
    1) создание и постоянное поддержание в Банке условий, при которых риски, связанные с безопасностью информационных активов, находятся под контролем и являются управляемыми;
    2) обеспечение соответствия требованиям законодательства, регулирующих органов, отраслевых стандартов и лучших практик в области информационной безопасности;
    3) обеспечение непрерывности бизнес-процессов, устойчивого функционирования и развития Банка;
    4) укрепление доверия к Банку со стороны клиентов, контрагентов, партнеров, инвесторов и общества в целом, повышение его рейтинга и инвестиционной привлекательности.

§3. Задачи системы управления информационной безопасностью

19. Для достижения поставленных целей системы управления информационной безопасностью Банк обеспечивает эффективное выполнение следующих задач:
    1) идентификацию и классификацию информационных активов;
    2) оценку, обработку и мониторинг рисков информационной безопасности
    3) определение и документирование применимых требований к информационной безопасности и процедур их обеспечения;

4) обучение работников Банка процедурам обеспечения информационной безопасности, повышение их осведомленности и установление ответственности по вопросам информационной безопасности;
5) регулярную оценку соответствия системы управления информационной безопасностью применимым внутренним и внешним требованиям путем проведения внутренних аудитов и анализа со стороны руководства Банка;
6) информирование заинтересованных сторон о подходах Банка к обеспечению информационной безопасности, управлению инцидентами, а также о результатах независимых аудитов информационной безопасности Банка.

§4. Принципы построения системы управления информационной безопасностью

20. Построение и функционирование системы управления информационной безопасностью в Банке осуществляется в соответствии со следующими основными принципами:
1) законность - все действия, предпринимаемые для обеспечения информационной безопасности Банка, осуществляются на основании действующего законодательства с применением разрешенных методов, средств и механизмов управления, обеспечения и контроля информационной безопасности;
2) адекватность - принимаемые меры информационной безопасности определяются на основе анализа рисков с учетом потребностей бизнеса и уровня угроз;
3) непрерывность функционирования - обеспечивается устойчивость, надежность и доступность функционирования организационных и технических мер управления информационной безопасностью;
4) персональная ответственность - каждый работник Банка несет ответственность за выполнение обязанностей и соблюдение требований, возложенных на него в рамках функционирования системы управления информационной безопасностью;
5) минимизация полномочий - доступ к информации предоставляется работникам Банка в объеме, определяемом их должностными функциями и обязанностями;
6) исключение конфликта интересов - обязанности работников распределяются таким образом, чтобы исключить возможность конфликта интересов. В частности, ни один работник не должен обладать полномочиями, позволяющими ему единолично выполнять критически важные операции;
7) комплексность - построение системы управления информационной безопасностью основывается на согласованном применении различных мер управления информационной безопасностью, охватывающих все ключевые каналы реализации угроз и исключающих уязвимости на стыках компонентов.

§5. Область действия системы управления информационной безопасностью

21. Область действия системы управления информационной безопасностью определяется как совокупность процессов, ресурсов и субъектов, на которые распространяются требования по обеспечению информационной безопасности в рамках деятельности Банка.
22. Область действия системы управления информационной безопасностью включает следующие элементы:
    1) бизнес-процессы, обеспечивающие устойчивое функционирование и достижение стратегических целей Банка;
    2) информационные активы, включая электронные информационные ресурсы, базы данных, документы, программное обеспечение;
    3) информационную инфраструктуру, включая центры обработки данных, серверы, сети, устройства хранения, пользовательские устройства, каналы связи и иные технические средства, обеспечивающие обработку, хранение и передачу информации;
    4) работников Банка, имеющих доступ к информационным активам, включая стажеров и практикантов;
    5) внутренние процессы и процедуры, регламентирующие обработку информации, управление доступом, реагирование на инциденты, аудит и оценку эффективности;
    6) контрагентов, поставщиков и внешние ИТ-сервисы, если они вовлечены в обработку, передачу или хранение информации Банка.
23. Область действия подлежит регулярному пересмотру и при необходимости уточняется.

§6. Реализация системы управления информационной безопасностью

24. Построение и развитие системы управления информационной безопасностью осуществляется как циклический процесс на основе модели непрерывного улучшения Деминга – Шухарта (PDCA: Plan – Do – Check – Act), включающей следующие этапы:
    1) планирование («Plan») - определение области действия системы управления информационной безопасностью, формализация подхода к управлению рисками информационной безопасности, определение и распределение ресурсов, разработка мер по управлению информационной безопасностью;
    2) выполнение («Do») - реализация мер, разработанных на этапе планирования, а также выполнение решений, принятых по результатам предыдущих циклов; проведение оценки и обработки рисков информационной безопасности;
    3) проверка («Check») - оценка результатов функционирования системы управления информационной безопасностью с целью получения уверенности в ее эффективности, адекватности существующим угрозам и соответствия внутренним и внешним факторам, влияющим на деятельность Банка;
    4) корректировка («Act») – принятие решений о корректирующих действиях и действиях по реализации выявленных возможностей для улучшения, направленных на постоянное улучшение системы

управления информационной безопасностью, на основе результатов этапа «проверка».

§7. Направления развития и улучшения системы управления информационной безопасностью

25. Настоящая Политика определяет следующие основные направления постоянного развития и улучшения системы управления информационной безопасностью:

1) организация деятельности по обеспечению информационной безопасности - определение и распределение ролей, обязанностей и полномочий по обеспечению информационной безопасности в Банке, а также доведение этой информации до всех заинтересованных сторон;
2) управление документированной информацией - разработка, согласование, утверждение, хранение, передача и уничтожение документов, относящихся к системе управления информационной безопасностью;
3) управление рисками информационной безопасности - идентификация, оценка, обработка и мониторинг рисков информационной безопасности;
4) оценка эффективности - проведение мониторинга, измерений, анализа и оценки эффективности системы управления информационной безопасностью, включая внутренний аудит и анализ со стороны руководства;
5) обеспечение безопасности персонала - реализация мер по соблюдению требований информационной безопасности при приеме на работу, в процессе трудовой деятельности, при переводе и увольнении;
6) управление информационными активами - идентификация, классификация, установление правил допустимого использования и обязанностей по защите информационных активов;
7) управление доступом - предоставление доступа к информационным активам исключительно авторизованным пользователям, предотвращение несанкционированного доступа;
8) применение криптографической защиты - использование криптографических методов для обеспечения конфиденциальности, целостности и подлинности информации;
9) физическая безопасность и защита от воздействия окружающей среды - предотвращение несанкционированного физического доступа, повреждения, кражи, а также защита от факторов, способных нарушить бизнес-процессы Банка;
10) безопасная эксплуатация информационной инфраструктуры - обеспечение корректной и безопасной эксплуатации средств обработки информации, защита от вредоносных программ, резервное копирование, ведение и защита журналов аудиторского следа, управление уязвимостями и программным обеспечением;
11) управление сетевой безопасностью - обеспечение безопасности информации при ее передаче как внутри, так и за пределы Банка;

12) обеспечение информационной безопасности на всех этапах жизненного цикла информационных систем - обеспечение соблюдения требований к информационной безопасности при их проектировании, разработке, внедрении, эксплуатации, модификации и выводе из эксплуатации, включая защиту тестовых данных;

13) взаимоотношение с поставщиками - установление и контроль требований к информационной безопасности в соглашениях и договорах с поставщиками, имеющими доступ к информационным активам Банка;

14) управление инцидентами информационной безопасности - обеспечение последовательного и эффективного подхода к мониторингу, выявлению, реагированию и расследованию инцидентов информационной безопасности;

15) информационная безопасность в управлении непрерывностью бизнеса - обеспечение целостности и доступности информации и средств ее обработки при реализации планов по обеспечению непрерывности и восстановлению деятельности;

16) соблюдение требований законодательства, регулирующих органов, отраслевых стандартов, договорных обязательств, а также положений настоящей Политики и иных внутренних нормативных документов Банка по информационной безопасности.

26. Требования информационной безопасности уточняются и детализируются во внутренних нормативных документах Банка, разрабатываемых в рамках системы управления информационной безопасностью на основе настоящей Политики.

§8. Требования к управлению доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах Банка

27. Управление доступом к информации направлено на обеспечение конфиденциальности, целостности и доступности информационных активов Банка, предотвращение несанкционированного доступа, изменения или уничтожения информации.

28. Общий подход к управлению доступом основывается на принципах:

1) минимальных привилегий - предоставление доступа только в объеме, необходимом для выполнения должностных обязанностей;

2) разграничения прав доступа - использование ролевой модели доступа, основанной на должностных и функциональных обязанностях, категориях пользователей и уровнях конфиденциальности информации;

3) непрерывного контроля и пересмотра - регулярный пересмотр актуальности прав доступа и своевременное их изменение или отзыв;

4) персонифицированного доступа - все действия в информационных системах осуществляются только с использованием персонализированных учетных записей;

5) фиксации событий доступа - ведение журналов доступа и действий пользователей для последующего анализа и расследования инцидентов;

29. Требования к процессам управления доступом включают:

1) формализацию и документирование процедур предоставления, изменения и отзыва прав доступа, включая согласование с владельцем информационного актива;
2) использование автоматизированных средств управления доступом, по возможности интегрированных с системами управления идентификацией и аутентификацией;
3) обязательное проведение периодических проверок соответствия фактического доступа утвержденным правам и ролям пользователей;
4) регистрацию всех действий по управлению доступом, включая даты, основания и ответственных лиц;
5) обеспечение специальных процедур доступа для ситуаций, связанных с инцидентами, авариями или необходимостью экстренного доступа (в т.ч. привилегированный доступ).

30. Управление доступом осуществляется в соответствии с требованиями настоящей Политики, внутренних нормативных документов Банка и применимых международных стандартов в области информационной безопасности.

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

31. Мониторинг деятельности по обеспечению информационной безопасности направлен на контроль выполнения установленных требований системы управления информационной безопасностью, достижение целей (задач) информационной безопасности и своевременное выявление отклонений, инцидентов или неэффективных мер управления информационной безопасностью.

32. Общий подход к мониторингу основывается на следующих принципах:

1) регулярности и системности - мониторинг осуществляется на постоянной основе в рамках утвержденных процессов и процедур;
2) доказательности - все результаты мониторинга должны быть зафиксированы, подтверждены и доступны для анализа;
3) объективности и независимости - анализ данных проводится беспристрастно, при необходимости - с участием независимых специалистов или структурных подразделений Банка;
4) ориентации на улучшение - результаты мониторинга используются для инициирования корректирующих и предупреждающих действий.
5) Требования к процессам мониторинга включают:
6) организацию и выполнение мониторинга силами Управления информационной безопасности Департамента Безопасности с участием других заинтересованных структурных подразделений Банка;
7) сбор, хранение и анализ данных о реализации мер управления информационной безопасностью, инцидентах, отклонениях и несоответствиях;

8) представление результатов мониторинга в виде отчетов и аналитических материалов для руководства и регулирующих органов;
9) использование автоматизированных средств контроля, включая системы централизованного сбора и корреляции событий безопасности (SIEM);
10) документирование всех этапов мониторинга, включая примененные методы, выявленные проблемы и принятые корректирующие меры.

33. Мероприятия по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов направлены на обеспечение готовности к реагированию, минимизацию ущерба и предотвращение повторных инцидентов информационной безопасности.

34. Общий подход к выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности основывается на следующих принципах:
1) проактивности - использование превентивных мер и раннего обнаружения угроз для недопущения реализации атак;
2) своевременности реагирования - оперативное выполнение необходимых действий при возникновении инцидентов;
3) комплексности - рассмотрение инцидентов с учетом всех возможных факторов и уязвимостей;
4) доказательности и прослеживаемости - фиксация всей информации об инцидентах для анализа, отчетности и последующего улучшения;
5) непрерывности совершенствования - использование полученного опыта для повышения устойчивости Банка к угрозам информационной безопасности.

35. Требования к мероприятиям по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности включают:
1) идентификацию и анализ угроз - сбор и обработку информации о потенциальных и реальных угрозах с использованием технических и аналитических средств, в том числе систем обнаружения вторжений, SIEM, отчетов о внешней и внутренней активности;
2) предотвращение и противодействие атакам - реализацию превентивных мер управления информационной безопасностью, настройку и использование средств защиты (межсетевые экраны, антивирусы, средства обнаружения и предотвращения вторжений и др.), а также применение процедур быстрого реагирования;
3) расследование инцидентов - установление причин, масштабов, последствий инцидентов, а также разработку корректирующих мер;
4) ведение журнала учета инцидентов - регистрация всех инцидентов информационной безопасности с обязательным указанием времени обнаружения, характеристик, причин, принятых мер, вовлеченных лиц и результатов реагирования;
5) анализ тенденций и повторяющихся инцидентов - использование накопленной информации для выявления закономерностей, анализа

динамики угроз, актуализации мер управления информационной безопасностью и корректировки применяемых подходов.

36. Мониторинг деятельности по обеспечению информационной безопасности, а также выявление и анализ угроз, противодействие атакам и расследование инцидентов информационной безопасности осуществляются в соответствии с требованиями настоящей Политики, внутренних нормативных документов Банка и применимых международных стандартов в области информационной безопасности.

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

37. Сбор, консолидация и хранение информации об инцидентах информационной безопасности направлены на обеспечение полноты и достоверности сведений, необходимых для анализа причин, оценки ущерба, повышения эффективности реагирования и предупреждения повторных инцидентов.

38. Общий подход к сбору, консолидации и хранения информации об инцидентах информационной безопасности основывается на следующих принципах:

1) достоверности - сведения об инцидентах должны быть точными, полными и подтвержденными источниками, зафиксированными в системе учета;
2) оперативности - информация должна собираться, обрабатываться и консолидироваться без задержек, в пределах установленных сроков, соответствующих критичности инцидента;
3) защищенности - информация об инцидентах подлежит защите от несанкционированного доступа, изменений и удаления, в том числе с использованием технических и организационных мер;
4) прослеживаемости - все изменения и действия с данными об инцидентах должны регистрироваться и быть доступны для последующего анализа;
5) структурированности - используемые формы и форматы сбора и хранения информации стандартизированы и обеспечивают единообразие учета.

39. Требования к процессам сбора, консолидации и хранения информации об инцидентах включают:

1) использование автоматизированных систем регистрации и учета инцидентов, обеспечивающих централизованное хранение и возможность анализа данных;
2) формализацию процедуры сбора первичной информации, включая назначение ответственных лиц, сроки предоставления сведений и перечень обязательных параметров (тип, источник, время обнаружения, описание, классификация по критичности, принятые меры и пр.);
3) ведение единого журнала учета инцидентов информационной безопасности, содержащего сведения о всех зафиксированных инцидентах с возможностью последующего поиска и анализа;
4) хранение информации об инцидентах в течение установленного срока в соответствии с внутренними нормативными документами Банка и требованиями законодательства Республики Казахстан;

5) обеспечение доступа к информации об инцидентах строго в пределах должностных и функциональных обязанностей, с применением механизмов разграничения прав и ведением журналов аудиторского следа.

40. Информация об инцидентах информационной безопасности используется для анализа причин и последствий инцидентов, а также для принятия решений об улучшении процессов обеспечения информационной безопасности.

41. Сбор, консолидация и хранение информации об инцидентах информационной безопасности осуществляются в соответствии с требованиями настоящей Политики, внутренних нормативных документов Банка и применимых международных стандартов в области информационной безопасности.

§11. Требования к проведению анализа информации об инцидентах информационной безопасности

42. Анализ информации об инцидентах информационной безопасности направлен на установление причин, выявление уязвимостей, оценку ущерба, формирование корректирующих и предупреждающих мер, а также на повышение устойчивости системы управления информационной безопасностью к повторным инцидентам.

43. Общий подход к анализу инцидентов информационной безопасности основывается на следующих принципах:

1) достоверности - используются только подтвержденные и проверенные данные, полученные в ходе регистрации и расследования инцидентов;
2) системности - инциденты рассматриваются не изолированно, а с учетом возможных взаимосвязей, повторяемости и среды функционирования Банка;
3) ориентированности на устранение причин - основной целью анализа является не только устранение последствий, но и предотвращение повторного возникновения аналогичных инцидентов;
4) документируемости - все этапы анализа подлежат фиксации с указанием выводов и принятых решений.

44. Требования к процессу анализа инцидентов информационной безопасности включают:

1) проведение анализа в установленные сроки, с учетом классификации и приоритизации инцидента;
2) установление причин и факторов, способствовавших возникновению инцидента, включая человеческие, организационные, технические и внешние;
3) определение последствий инцидента, включая оценку ущерба, влияние на бизнес-процессы и нарушение требований информационной безопасности;
4) формирование предложений по устранению выявленных уязвимостей, корректирующих мерах, а также предупреждению аналогичных инцидентов в будущем;
5) представление результатов анализа инцидентов для рассмотрения руководством Банка и иными заинтересованными сторонами;

6) использование накопленных аналитических материалов для актуализации системы управления рисками и улучшения системы управления информационной безопасностью.

45. Анализ информации об инцидентах осуществляется в соответствии с требованиями настоящей Политики, внутренними нормативными документами Банка и международными стандартами в области информационной безопасности.

Глава 4. Заключительные положения

46. Настоящая Политика и внутренние нормативные документы Банка по информационной безопасности, обязательны для исполнения всеми работниками Банка, стажерами, практикантами, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным активам Банка, в части их касающейся.

47. Ответственность за обеспечение информационной безопасности при исполнении возложенных на них должностных функций и обязанностей возлагается на всех работников Банка.

48. Ответственность за ненадлежащее исполнение и нарушение работниками структурных подразделений Банка требований информационной безопасности возлагается на руководителей соответствующих структурных подразделений Банка.

49. Ответственность за ознакомление работников Банка с настоящей Политикой возлагается на Департамент HR.

50. Пересмотр положений настоящей Политики осуществляется при необходимости, но не реже одного раза в два года в соответствии с порядком, установленным в Банке.

51. Внеплановый пересмотр настоящей Политики осуществляется в случае:

1) существенных изменений законодательства Республики Казахстан, затрагивающих деятельность Банка, организационной структуры или бизнес-процессов Банка;

2) выявления существенных недостатков при выполнении мероприятий, регламентированных настоящей Политикой, а также противоречий ее положений с другими внутренними нормативными документами Банка.

52. Во всем, что прямо не урегулировано настоящим Положением, необходимо руководствоваться требованиями действующего законодательства Республики Казахстан и внутренних нормативных документов Банка.

53. Изменения в настоящую Политику могут быть утверждены только решением Совета Директоров.