Утверждена
Советом директоров
АО «Amaranth Capital»
(Протокол №8-2025от 15.10.2025г.)

Акционерное общество «Amaranth Capital»

Политика информационной безопасности АО «Amaranth Capital»

Алматы, 2025

Содержание

Политика
информационной безопасности
АО «Amaranth Capital»

Глава 1. Общие положения

1. Настоящая Политика информационной безопасности АО «Amaranth Capital» (далее – Политика) разработана в соответствии с действующим законодательством Республики Казахстан, требованиями Национального Банка Республики Казахстан, Уставом АО «Amaranth Capital» (далее – Компания) и международным стандартом ISO/IEC 27001.
2. Настоящая Политика является внутренним документом Компании, определяющим единый подход, принципы и основные правила для обеспечения информационной безопасностью (далее – ИБ).
3. Компания обеспечивает создание, надлежащий уровень функционирования, развития и улучшения Системы управления информационной безопасности (далее – СУИБ), являющейся частью общей системы управления Компании, предназначенной для управления процессом обеспечения ИБ.
4. Участниками СУИБ Компании являются:
   1) Совет Директоров;
   2) Правление;
   3) Отдел информационной безопасности.
5. СУИБ обеспечивает защиту информационных активов Компании, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Компании.
6. Настоящая Политика определяет:
   1) цели, задачи и основные принципы построения СУИБ;
   2) область действия СУИБ;
   3) требования к доступу к создаваемой, хранимой и обрабатываемой информации в информационных системах (далее – ИС) Компании, организации и мониторингу информации и доступа к ней;
   4) требования к осуществлению мониторинга деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ;
   5) требования к осуществлению сбора, консолидации и хранения информации об инцидентах ИБ;
   6) требования к проведению анализа информации об инцидентах ИБ;
   7) ответственность работников Компании за обеспечение ИБ при исполнении возложенных на них функциональных обязанностей.
7. Настоящая Политика является внутренним документом Компании, действующим наравне с другими политиками, принятыми Компанией в установленном

порядке.

8. Положения настоящей Политики обязательны к исполнению всеми работниками Компании, нештатными работниками, а также доводится до сведения клиентов, контрагентов и иных третьих лиц, имеющих доступ к информационным активам и внутренним документам Компании, в той части, которая непосредственно взаимосвязана с Компанией и их деятельностью.

9. Ознакомление с настоящей Политикой является обязательным для каждого работника при приёме на работу, а также для третьих лиц, имеющих доступ к информационным активам и внутренним документам Компании.

Глава 2. Основные термины и принятые сокращения

10. В настоящей Политике используются следующие сокращения и определения:
    1) **актив** – все, что имеет ценность для Компании и находится в ее распоряжении;
    2) **бизнес-владелец ИС/ИПС** – подразделение (работник) Компании, являющееся (являющийся) владельцем основного бизнес-процесса, который автоматизирует информационная система;
    3) **владелец бизнес-процесса** – подразделение (работник) Компании, отвечающее (отвечающий) за жизненный цикл конкретного бизнес-процесса и координацию деятельности подразделений Компании, вовлеченных в бизнес-процесс;
    4) **возможность применения (доступность)** – свойство доступности и готовности к использованию по авторизованному запросу;
    5) **доступ (доступ к информации)** – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации;
    6) **защита информации** – комплекс мероприятий, обеспечивающих информационную безопасность;
    7) **информационная безопасность (ИБ)** – состояние защищенности электронных информационных ресурсов, информационных систем и информационно- коммуникационной инфраструктуры от внешних и внутренних угроз;
    8) **информационный актив** – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;
    9) **информационная инфраструктура** – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;
    10) **информационная система** – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные

технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

11) **инцидент информационной безопасности** – отдельно или серийно возникающие сбой 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;
12) **конфиденциальность** – свойство, указывающее, что информация остается недоступной или нераскрытой для неавторизованных частных и юридических лиц или процессов;
13) **Правление** – коллегиальный орган Компании, уполномоченный принимать решения по задачам обеспечения информационной безопасности;
14) **риск ИБ** – риск возникновения ущерба вследствие нарушения целостности, конфиденциальности и доступности информационных активов Компании, возникшего вследствие преднамеренного деструктивного воздействия со стороны работников Компании и (или) третьих лиц;
15) **событие информационной безопасности** – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации;
16) **третьи лица (третья сторона)** – нештатные работники Компании, а также юридические лица (организации), клиенты Компании, имеющие право доступа к информационным активам Компании.
17) **угроза информационной безопасности** – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;
18) **целостность** – свойство сохранения полноты и точности.

Глава 3. Цели, задачи и основные принципы построения СУИБ

11. Целью СУИБ Компании является создание и постоянное поддержание в Компании условий, при которых риски ИБ контролируются и находятся в приемлемом уровне.

12. Достижение данной цели позволяет, но не ограничивает:
    1) соответствовать требованиям законодательства Республики Казахстан, регулятора в лице Национального Банка Республики Казахстан;
    2) увеличить прибыль и получить дополнительные возможности, связанные с осуществляемой Компанией деятельностью;
    3) защитить информационные активы Компании, от реализации различных типов угроз (внешних и внутренних, умышленных и непреднамеренных);
    4) обеспечить непрерывность деятельности Компании;
    5) повысить культуру ИБ персонала Компании.

13. В процессе обеспечения должного уровня ИБ Компания руководствуется следующими основными принципами:
    1) вовлеченность высшего руководства Компании в процесс управления ИБ. Деятельность по обеспечению ИБ инициирована и контролируется высшим руководством Компании. Координация деятельности по обеспечению ИБ осуществляется в рамках Правления Компании. Высшее руководство демонстрирует приверженность СУИБ и выполняет те же правила по обеспечению ИБ, что и все работники Компании;
    2) реагирование на инциденты ИБ. Компания стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения ИБ;
    3) осведомлённость в вопросах обеспечения ИБ. Требования в области ИБ доводятся до сведения штатных, нештатных (стажеров, практикантов) работников Компании, клиентов и контрагентов в части осуществляемой ими деятельности;
    4) компетентность персонала. Компания тщательно производит процедуру найма работников, повышает квалификацию, на системной основе осуществляет информирование и обучение работников по вопросам обеспечения ИБ;
    5) персональная ответственность. Работники Компании несут персональную ответственность за соблюдение требований ИБ. Обязанности по обеспечению ИБ включаются в трудовые договоры, а также в договоры с контрагентами;
    6) управление корпоративными рисками. Управленческие решения в Компании (в том числе и в области ИБ) принимаются на основании результатов оценки рисков;
    7) согласованность действий и решений по обеспечению ИБ с поставленными стратегическими целями Компании. Деятельность по обеспечению ИБ учитывает контекст управления стратегическими рисками;
    8) соответствие требованиям законодательства Республики Казахстан, а также условиям заключенных договоров с клиентами и контрагентами. Компания реализует меры обеспечения ИБ в строгом соответствии с действующим законодательством Республики Казахстан и договорными обязательствами;
    9) соответствие СУИБ высоким стандартам и лучшим практикам. Функционирование СУИБ строится в соответствии с применимыми требованиями стандартов Республики Казахстан, международных стандартов, а также лучших мировых практик;
    10) экономическая обоснованность. Применяемые организационные и технические меры выбираются исходя из требований к осуществляемой Компанией деятельности на основе анализа рисков ИБ и затрат на внедрение и сопровождение. Проводится периодическая оценка эффективности используемых мер;
    11) документированность требований ИБ. Компания стремится, чтобы все требования в области ИБ были зафиксированы во внутренних документах Компании, утвержденных уполномоченным органом Компании;

12) предоставление минимально необходимых прав доступа. Работникам Компании, третьим лицам предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств. При этом Компания стремится предоставлять права доступа таким образом, чтобы выполнение особо важной (критичной) операции осуществлялось с участием как минимум 2 (двух) работников Компании.

Глава 4. Область действия СУИБ

14. Компания устанавливает границы СУИБ с целью определения, какую информацию следует защищать. Такая информация потребует защиты, независимо от того, добавлена ли она дополнительно для хранения, обрабатывается или перемещается в область действия СУИБ или из нее. Факт нахождения какой-либо информации за пределами области действия СУИБ не означает, что к ней не будут применены меры безопасности – это означает только, что ответственность по применению мер безопасности будет передана третьей стороне, которая управляет этой информацией.

15. Область действия СУИБ охватывает:
    1) все бизнес-процессы Компании;
    2) все структурные подразделения Компании;
    3) все офисы Компании.

16. Исключений из области действия СУИБ Компании нет.

Глава 5. Требования к обеспечению информационной безопасности

§1. Требования по категорированию информационных активов

17. Компания осуществляет категорирование информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности, хранимой и обрабатываемой в них информации.

18. Компания формирует внутренний документ, в котором составляет перечень критичных информационных активов с указанием их владельцев.

19. Компания обеспечивает ИБ информационных активов, отнесенных к категории критичных в соответствии с требованиями законодательства РК.

20. Компания разрабатывает Перечень защищаемой информации и Правила обращения с ней, описывающий порядок определения защищаемой информации и ее категорирование на основе оценки возможного ущерба путем разделения на критичную и некритичную.

§2. Требования к организации доступа к информационным активам

21. Компания поддерживает порядок предоставления физического доступа к информационным активам Компании согласно внутренним документам

Компании.

22. Физический доступ к средствам обработки информации предоставляется только авторизованным работникам на основании Приказа Председателя Правления Компании/лица, исполняющего его обязанности.

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

24. Для предоставления доступа к информационным активам Компании, отнесенным к категории критичных информационных активов, Компания формирует и внедряет роли для обеспечения соответствия прав доступа пользователей ИС их функциональным обязанностям.

25. Компания разрабатывает внутренний документ, описывающий процесс создания и использования матриц доступа в ИС Компании.

§3. Требования к обеспечению безопасности информационной инфраструктуры

26. Компанией проводятся организационные мероприятия и (или) устанавливаются программно-технические средства, снижающие риск доступа к информационной инфраструктуре неавторизованных устройств либо устройств, настройки которых противоречат установленному внутренним документом Компании порядку обеспечения ИБ.

27. Для каждой ИС или информационной подсистемы (далее – ИПС) определяется бизнес-владелец.

28. При разработке технических заданий на создание (модернизацию) объектов информационной инфраструктуры бизнес-владелец ИС/ИПС учитывает требования к ИБ.

29. Компания обеспечивает резервное хранение данных критичных ИС, их файлов и настроек, которое обеспечивает восстановление работоспособной копии ИС.

30. Компания обеспечивает антивирусную защиту информационной инфраструктуры.

31. Компания обеспечивает уничтожение защищаемой информации методами, исключающими ее восстановление, с использованием любого из следующих методов уничтожения информации в зависимости от типа носителя: а) физическое уничтожение носителя информации; б) программное уничтожение электронной информации штатными средствами операционной системы.

32. Компания обеспечивает своевременную установку обновлений безопасности информационных систем. Обновления безопасности информационных систем, устраняющие критичные уязвимости, устанавливаются не позднее одного месяца со дня их публикации и распространения производителем.

33. Компания обеспечивает физическую безопасность центров обработки данных Компании.

34. Компанией определяется перечень программного обеспечения и оборудования, разрешенных к использованию в Компании.

35. Внутренними документами Компании определяются организационные и технические меры, обеспечивающие защиту рабочих станций и мобильных устройств Компании, а также носителей информации и сетевых ресурсов.

§4. Требования к осуществлению мониторинга деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ

36. Компанией проводится мониторинг деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ.

37. Компанией проводится мониторинг событий ИБ и управление инцидентами ИБ.

38. Подразделение Компании, осуществляющее мониторинг, наделяется полномочиями по введению дополнительных контролей, частичную или полную остановку бизнес-процесса в случае выявления инцидента ИБ.

39. Компанией определяются перечень событий ИБ, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы.

40. Компанией определяется порядок отнесения события ИБ к инцидентам ИБ.

§5. Требования к средствам криптографической защиты информации

41. Компания определяет порядок использования средств криптографической защиты информации с указанием применимых средств криптографической защиты информации, их назначения, реализованных в них криптографических алгоритмов, наименовании ИС, владельца ИС.

42. Процесс внедрения и поддержки средств криптографической защиты информации согласовывается бизнес-владельцем ИС с Отделом информационной безопасности.

§6. Требования к обеспечению информационной безопасности при доступе третьих лиц к информационным активам

43. Компания предусматривает требования к ИБ при доступе к информационным активам третьих лиц, не являющихся работниками Компании.

44. Доступ третьих лиц к информационным активам Компании предоставляется на период и в минимально достаточном объеме, необходимых для проведения работ на основании соглашения о соблюдении требований к ИБ, за исключением случаев, предусмотренных законодательством Республики Казахстан. При установлении деловых отношений в соглашениях о соблюдении требований к ИБ, заключаемых с третьими лицами, содержатся положения о конфиденциальности, условия о возмещении ущерба, возникшего вследствие нарушения ИБ, а также сбоев в работе ИС и нарушения их безопасности,

вызванных вмешательством третьих лиц.

45. Предусматриваются следующие организационные и/или программно-технические меры по контролю деятельности третьих лиц:

1) проверка результата деятельности третьих лиц;

2) осуществление деятельности третьих лиц в присутствии работников Компании;

3) ведение аудиторского следа по действиям третьих лиц;

§7. Требования к проведению внутренних проверок состояния информационной безопасности

46. Состояние ИБ оценивается путем проведения проверок деятельности структурных подразделений Компании:

Службой внутреннего аудита – в рамках годового плана аудиторских проверок в соответствии с внутренними документами Компании, регламентирующими организацию системы внутреннего аудита Компании.

На ежегодной основе Компания подвергает внешнему аудиту процессы обеспечения информационной безопасности ключевых информационных систем.

47. По результатам проверки составляется отчет с приложением материалов проверки, который доводится до сведения проверяемого подразделения Компании.

Глава 6. Распределение ответственности Компании за обеспечение ИБ

48. Совет директоров Компании:
1) утверждает основные принципы управления ИБ;
2) утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация),
3) порядок работы с защищаемой информацией.

49. Правление Компании:
1) осуществляет стратегическое планирование, утверждение внутренних документов, регламентирующих процесс управления ИБ;
2) координирует деятельность всех структурных подразделений Компании для организации и поддержания соответствующего уровня ИБ;
3) отвечает за общее состояние СУИБ в Компании, утверждает бюджет системы обеспечения безопасности.

50. В случае, если отдельные функции обеспечения ИБ Компании переданы сторонним организациям Председатель Правления Компании является ответственным за обеспечение ИБ.

51. Отдел информационной безопасности несёт ответственность за:

1) выбор, внедрение, администрирование, контроль и улучшение принятых в Компании мер и средств защиты информации в ИТ-инфраструктуре;
2) осуществление мониторинга режима ИБ;
3) соблюдение требований ИБ во всех направлениях деятельности Компании;
4) надлежащий контроль и эффективность предпринимаемых мер по ИБ;
5) своевременную реализацию технических мер, обеспечивающих ИБ ИС и технических средств;
6) разработку внутренних документов в части регламентации программно-технических мер, обеспечивающих функционирование, конфиденциальность, целостность и доступность информационных активов.

52. Отдел рисков несет ответственность за внедрение, постоянное развитие и применение системы управления рисками ИБ.

53. Служба внутреннего аудита проводит оценку состояния СУИБ Компании в соответствии с внутренними документами Компании, регламентирующими организацию системы внутреннего аудита Компании.

54. Главный специалист комплаенс-контроля и финансового мониторинга совместно с Юридическим отделом Компании определяют виды информации, подлежащие включению в перечень защищаемой информации, составляющих служебную, коммерческую или иную охраняемую законом тайну.

55. Юридический отдел Компании осуществляет правовую экспертизу внутренних документов Компании по вопросам обеспечения ИБ.

56. Руководители структурных подразделений Компании несут ответственность за доведение и исполнение настоящей Политики, обеспечивают ознакомление работников с внутренними документами Компании, содержащими требования к ИБ, несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях Компании, а также за доведение до работников о необходимости извещения своего непосредственного руководителя и начальника Отдела информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

57. Все работники структурных подразделений Компании:
1) несут дисциплинарную ответственность за соблюдение требований к ИБ, принятых в Компании;
2) контролируют исполнение требований к ИБ третьими лицами, с которыми они взаимодействуют в рамках своих функциональных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;
3) незамедлительно извещают своего непосредственного руководителя и начальника Отдела информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.
4) обязаны проходить обучение или переподготовку и переподготовку в целях регулярного получения информации о требованиях процедур по ИБ.

Глава 7. Заключительные положения

58. Контроль за исполнением настоящей Политики возлагается на Члена Правления ответственного за ИТ и ИБ в Компании.
59. Актуализация настоящей Политики входит в обязанности Отдела информационной безопасности.
60. Настоящая Политика подлежит пересмотру и актуализации при необходимости.
61. Настоящая Политика вступает в силу с момента ее утверждения Советом Директоров Компании.
62. С даты принятия настоящего решения Совета директоров признать утратившим силу Политику информационной безопасности АО «Amaranth Capital», утвержденную Советом директоров Общества (протокол №1-2025 от 21.04.2025г.)

Председатель Правления **Иваненко Н.В.**