УТВЕРЖДЕНО
Решением Совета директоров
АО «Инвестиционная
компания Standard»
№ 24 от «20» октября 2023 г.

Политика информационной безопасности АО «Инвестиционная компания Standard»

Алматы, 2023г.

Содержание

1. Общие положения

1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим и верхне-уровневым внутренним нормативным документом системы управления информационной безопасностью АО «Инвестиционная компания Standard» (далее - Общество), определяющим цели, задачи, область действия и участников системы управления информационной безопасностью Общества (далее - СУИБ). Подробные подходы и методы для каждого процесса информационной безопасности описаны в соответствующих процедурах.

2. Общество обеспечивает создание, функционирование, развитие и улучшение СУИБ, являющейся частью общей системы управления, предназначенной для управления процессом обеспечения информационной безопасности.

3. Общество обеспечивает создание подразделения по информационной безопасности, подразделения по информационным технологиям и подразделения по управлению рисками посредством их подчинения разным членам исполнительного органа Общества, или напрямую руководителю исполнительного органа Общества.

4. СУИБ обеспечивает защиту информационных активов Общества, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Общества.

5. Информационная безопасность Общества в сфере информатизации представляет собой состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации Общества и повлечь нанесение иного ущерба Обществу, ее акционерам, работникам или клиентам.

6. Политика разработана в соответствии с законодательством Республики Казахстан, в том числе нормативными правовыми актами, регулирующими требования к обеспечению информационной безопасности организаций, осуществляющих брокерскую и дилерскую деятельность на рынке ценных бумаг, с правом ведения счетов в качестве номинального держателя, деятельность по управлению инвестиционным портфелем, а также требованиями международных стандартов в области информационной безопасности.

7. На основании Политики разрабатывается ряд подчиненных внутренних нормативных документов, регламентирующих конкретные правила и методы обеспечения информационной безопасности. Такие документы могут дополнять и расширять требования Политики, но не могут вступать с ним в противоречие.

8. При разработке и применении средств и методов информационной безопасности должны учитываться требования договорных обязательств и контрактов, заключенных Обществом с третьими лицами.

9. Доступ третьих лиц к информационным ресурсам Общества осуществляется только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер.

10. Положения настоящей Политики обязательны для ознакомления и исполнения всеми работниками Общества, а также должны доводиться до сведения иных третьих лиц, имеющих доступ к информационным активам Общества, в той их части, которая непосредственно взаимосвязана с Обществом и их деятельностью.

11. В настоящей Политике используются следующие термины:

1) **информационный актив** – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки;

2) **привилегированная учетная запись** – учетная запись в информационной системе, обладающая привилегиями создания, удаления и изменения прав доступа учетных записей;
3) **бизнес-процесс** – совокупность взаимосвязанных мероприятий или задач, направленных на создание определенного продукта или услуги для внешнего или внутреннего потребителя;
4) **третьи лица** - лица, не являющиеся работниками Общества.
5) **УИТ –** Управление ИТ поддержки.
6) **СУИБ -** Система управления информационной безопасностью.

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

12. Целью СУИБ является повышение эффективности процессов обеспечения информационной безопасности, обеспечение требуемого уровня конфиденциальности, целостности и доступности информационных активов, и как следствие, снижение рисков информационной безопасности и связанного с ними ущерба.

13. К задачам СУИБ относятся:

1) категорирование информационных активов;
2) организация доступа к информационным активам;
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 активам;
8) проведение внутренних проверок состояния информационной безопасности.

14. Построение СУИБ и ее функционирование осуществляются в соответствии со следующими основными принципами:

1) 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 информационные активы Общества;
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 активов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
4) 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

технологических решений по обеспечению информационной безопасности не должна превышать стоимость защищаемых информационных активов;

5) адаптивность – определение и применение методов и средств защиты информационных активов в соответствии с их критичностью;

6) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем информационным активам, 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 Общества, 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

15. Областью действия СУИБ являются основные бизнес-процессы Общества, непосредственно ориентированные на предоставление услуг клиентам, представляющие ценность для клиентов и обеспечивающих получение прибыли, определённых в регламентах бизнес-процессов.

16. Объектами защиты являются информационные активы, необходимые для функционирования основных бизнес-процессов, к которым могут быть отнесены, но не ограничиваются:

1) индивидуальные устройства обработки информации;
2) носители информации;
3) периферийное компьютерное оборудование;
4) серверы;
5) сетевое оборудование;
6) аппаратура телефонии;
7) физические каналы связи;
8) базы данных;
9) виртуальные каналы связи;
10) системы виртуализации;
11) операционные системы;
12) программное обеспечение аппаратных средств;
13) прикладное программное обеспечение;
14) программное обеспечение телефонии.

4. Меры обеспечения информационной безопасности

17. Основными мерами по обеспечению информационной безопасности являются:

1) административно-правовые и организационные меры;
2) меры физической безопасности;
3) программно-технические меры.

18. Административно-правовые и организационные меры включают в себя (но не ограничены ими):

1) контроль исполнения требований законодательства Республики Казахстан, регламентирующего правила обращения с информацией, закрепляющего права и обязанности участников информационных отношений в процессе ее обработки и использования.
2) разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих настоящую Политику;
3) контроль соответствия бизнес-процессов требованиям настоящей Политики;
4) информирование и обучение работников Общества работе с информационными системами и требованиям информационной безопасности;
5) реагирование на инциденты, локализация и минимизация последствий;
6) управление доступом к создаваемой, хранимой и обрабатываемой информации в информационных активах;
7) мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
8) сбор, консолидация и хранение информации об инцидентах информационной безопасности;
9) анализ информации об инцидентах информационной безопасности;
10) анализ новых рисков информационной безопасности;
11) проведение профилактических мер при приеме на работу, переводе и увольнении работников Общества.

19. Меры физической безопасности включают в себя (но не ограничены ими):

1) организацию пропускного и внутри объектового режимов;
2) построение периметра безопасности защищаемых объектов;
3) организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
4) организацию противопожарной безопасности охраняемых объектов;
5) контроль доступа работников Общества в помещения ограниченного доступа;
6) способы размещения рабочих станций работников Общества;
7) способы защиты рабочих станций от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб;
8) процедуры и периодичность технического обслуживания рабочих станций для обеспечения непрерывной доступности и целостности;
9) способы защиты рабочих станций мобильных пользователей, находящихся за пределами Общества;
10) способы гарантированного уничтожения информации при повторном использовании рабочих станций или выводе из эксплуатации носителей информации;
11) правила выноса рабочих станций за пределы рабочего места.

20. Программно-технические меры защиты включают (но не ограничены ими):

1) использование лицензионного или разрешенного программного обеспечения и сертифицированных средств защиты информации;
2) использование средств защиты периметра сети (firewall, IPS и т.п.);
3) применение комплексной антивирусной защиты;
4) использование средств информационной безопасности, встроенных в информационные системы;
5) обеспечение регулярного копирования и архивирования информации;
6) контроль за правами и действиями пользователей, в первую очередь привилегированных;
7) применение средств криптографической защиты информации;
8) обеспечение безотказной работы аппаратных средств;
9) журналирование событий;
10) мониторинг состояния критичных элементов информационной системы.

5. Ответственность работников Общества за обеспечение информационной безопасности при исполнении возложенных на них должностных обязанностей

21. Председатель Правления Общества обеспечивает создание, функционирование и улучшение системы управления информационной безопасностью, являющейся частью общей системы управления Общества, предназначенной для управления процессом обеспечения информационной безопасности.

22. Участниками СУИБ Общества являются:
1) Совет директоров;
2) Правление Общества;
3) Комитет по рискам;
4) Управление информационной безопасности (далее - УИБ);
5) Управление IT поддержи (далее - УИТ);
6) Управление рисков (далее - УР);
7) Административно-хозяйственное управление;
8) Юридическое управление;
9) Управление Комплаенс службы;
10) Служба внутреннего аудита;
11) Руководители структурных подразделений.
12) Бизнес-владельцы процессов и информационных систем.

23. Совет директоров утверждает политику информационной безопасности и перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, также информацию, охраняемой Законом Республики Казахстан «О рынке ценных бумаг», Законом Республики Казахстан «Об акционерных обществах» и порядок работы с защищаемой информацией.

24. Правление Общества утверждает внутренние нормативные документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется внутренними документами Общества.

25. Комитет по рискам принимает решения по вопросам обеспечения информационной безопасности и действует в рамках полномочий, предоставленных Правлением Общества.

26. УИБ в целях обеспечения конфиденциальности, целостности и доступности информации Общества осуществляет следующие функции:

1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений Общества по обеспечению

информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает политику информационной безопасности Общества;

3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности Общества;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности Общества, 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 Комитетом по рискам решения по вопросам информационной безопасности;

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

9) определяет требования по использованию привилегированных учетных записей;

10) обеспечивает проведение мероприятий по повышению осведомленности работников Общества в области информационной безопасности;

11) осуществляет мониторинг состояния системы управления информационной безопасностью Общества;

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

27. УИТ в целях соблюдения информационной безопасности осуществляет следующие функции:

1) разрабатывает и поддерживает актуальность схемы информационной инфраструктуры Общества;

2) обеспечивает предоставление доступа пользователям к информационным активам Общества в соответствии с установленными правилами;

3) обеспечивает формирование типовых настроек и конфигурирование системного и прикладного программного обеспечения Общества с учетом требований информационной безопасности;

4) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Общества (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с внутренними документами Общества;

5) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

28. Управление рисками в целях соблюдения информационной безопасности осуществляет следующие функции:

1) Анализ и выдача рекомендаций в подразделение УИБ и УИТ по развитию системы управления рисками информационных технологий и информационной безопасности, которая обеспечивает минимизацию рисков информационных технологий и информационной безопасности;

2) участие в оценке рисков информационных технологий и информационной безопасности;

3) участие в мониторинге уровня рисков информационных технологий и информационной безопасности;

4) анализ результатов оценки рисков информационных технологий и информационной безопасности, проводимых УИТ и УИБ;

5) участие в разработке и формировании реестра рисков, включающего риски информационных технологий и информационной безопасности;

6) участие в разработке методик и процедур по идентификации и оценке рисков информационных технологий и информационной безопасности;

7) участие в рабочей группе по формированию перечня критичных информационных активов с разработкой методик по категорированию информационных активов и порядком формирования/актуализации перечня критичных информационных активов Общества;

8) предоставление отчетности или иной информации по управлению рисками информационных технологий и информационной безопасности Совету директоров.

29. Административно-хозяйственное управление в целях соблюдения информационной безопасности осуществляет следующие функции:

1) обеспечивает подписание работниками Общества, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников Общества в области информационной безопасности;

3) уведомляет уполномоченный орган о назначении и увольнении работников подразделения по информационной безопасности.

4) реализует меры физической и технической безопасности в Обществе, в том числе организует пропускной и внутриобъектовый режим;

5) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Общества».

30. Юридическое управление осуществляет правовую экспертизу внутренних нормативных документов Общества по вопросам обеспечения информационной безопасности.

31. Управление комплаенс службы совместно с Юридическим управлением определяет виды информации, подлежащие включению в перечень защищаемой информации, предусмотренной пунктом 23 настоящей Политики.

32. Служба внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Общества в соответствии с внутренними нормативными документами Общества, регламентирующими организацию системы внутреннего аудита Общества.

33. Бизнес-владельцы информационных систем или подсистем:

1) отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, эксплуатации информационных систем и предоставлении продуктов и услуг клиентам и подразделениям Общества, а также при интеграции информационных систем с внешними информационными системами, включая информационные системы государственных органов;

2) формируют и поддерживают актуальность матриц доступа к информационным системам.

34. Руководители структурных подразделений Общества в целях соблюдения информационной безопасности осуществляет следующие функции:

1) обеспечивают ознакомление работников с внутренними нормативными документами

Общества, содержащими требования к информационной безопасности;

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях;

3) обеспечивают заключение соглашений о неразглашении конфиденциальной информации и включение условий об обеспечении информационной безопасности в соглашения, договоры на оказание услуг/выполнение работ в случаях, когда подразделение Общества выступает инициатором заключения таких соглашений, договоров

35. Работники структурных подразделений Общества в целях соблюдения информационной безопасности осуществляет следующие функции:

1) отвечают за соблюдение требований к информационной безопасности, принятых в Обществе;

2) контролируют исполнение требований к информационной безопасности третьими лицами, с которыми они взаимодействуют в рамках своих должностных обязанностей, в том числе путем включения указанных требований в соглашения, договоры с третьими лицами;

3) извещают своего непосредственного руководителя и УИБ обо всех подозрительных ситуациях и нарушениях при работе с информационными активами Общества.

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

36. Доступ к информации и информационным системам Общества предоставляется работникам в объеме, необходимом для исполнения их должностных обязанностей.

37. В информационных системах Общества используются только персонализированные пользовательские учетные записи пользователей.

38. Предоставление доступа к критичным информационным системам Общества производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их должностным обязанностям.

39. Доступ третьим лицам к информационным активам Общества 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.

40. Доступ к информационным системам Общества осуществляется путем идентификации и аутентификации пользователей информационных систем. Идентификация и аутентификация пользователей информационных систем Общества производится посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов многофакторной аутентификации, либо с использованием способов биометрической и (или) криптографической и (или) аппаратной аутентификации.

41. 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, утверждаемым руководителем УИТ по согласованию с руководителем УИБ.

42. Общество применяет все необходимые организационные и технические меры, обеспечивающие эффективность процесса управления доступом к информационным активам.

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

43. В целях обеспечения надлежащего мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности ответственные подразделения и органы Общества обеспечивают:

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 службы реагирования на инциденты информационной безопасности по вопросам применения стандартных процедур реагирования;

5) определение ответственных работников и (или) подразделений Общества, 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 службы реагирования на инциденты информационной безопасности полномочиями по введению дополнительных мер контроля по частичной или полной остановке бизнес-процессов в случае выявления инцидента информационной безопасности;

8) определение порядка информирования руководящих работников Общества, подразделений Общества 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.

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

44. Ответственные подразделения Общества обеспечивают 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. УИБ предоставляет, а УИТ обеспечивает хранение информации об инцидентах информационной безопасности, результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования, которое составляет не менее 5 (пяти) лет.

9. Требования к проведению анализа информации об инцидентах информационной безопасности

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 ответственные подразделения и органы Общества обеспечивают:

1) проведение анализа выявленных инцидентов информационной безопасности и нанесенного ими ущерба для рассмотрения на Комитете по рискам Общества, с целью оценки рисков информационной безопасности, корректировки методов и средств обеспечения информационной безопасности;

2) оценку эффективности с целью корректировки процесса реагирования на инциденты информационной безопасности;

3) пересмотр перечня событий информационной безопасности, подлежащих мониторингу, источников событий, периодичности, порядка и методов мониторинга событий информационной безопасности.

10. Ответственность

47. Все работники Общества несут персональную ответственность за свои действия при работе с информационными активами Общества и обращение с защищаемой информацией Общества, а также за выполнением требований информационной безопасности, установленных настоящей Политикой и внутренними нормативными документами, разработанными на её основе.

48. За нарушение требований настоящей Политики и документов, разработанных на её основе, предусмотрена ответственность в соответствии с внутренними нормативными документами Общества и действующим законодательством Республики Казахстан.

11. Заключительные положения

49. Все вопросы, не урегулированные настоящей Политикой, решаются в соответствии с законодательством Республики Казахстан, внутренними нормативными документами и решениями уполномоченных органов Общества, а также сложившейся практикой деятельности Общества.

50. Политика вступает в силу с даты утверждения Советом Директоров Общества и прекращает свое действие с момента признания ее утратившей силу Советом Директоров Общества.

51. Если в результате изменения законодательства Республики Казахстан отдельные нормы настоящей Политики вступают в противоречие с действующим законодательством Республики Казахстан, то до момента внесения изменений в Политику, необходимо руководствоваться действующим законодательством Республики Казахстан и Политикой в части, не противоречащей законодательству Республики Казахстан.

52. Пересмотр настоящей Политики осуществляется УИБ не реже одного раза в два года.