Одобрено
Протоколом Правления
№ 2023/21 от 30.10.2023г.

Утверждено
Протоколом заочного заседания
Совета Директоров
№ 5-2023 от 14.11.2023г.

Политика информационной безопасности АО «СК «Sinoasia B&R (Синоазия БиЭндАр)»

1. Общие положения

1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом системы управления информационной безопасности АО «СК «Sinoasia B&R (Синоазия БиЭндАр)» (далее – Компания), определяющим цели, задачи и область действия системы управления информационной безопасностью (далее – СУИБ) Компании.

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

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

4. Политика разработана в соответствии с законодательством Республики Казахстан, в том числе нормативными правовыми актами, регулирующими требования к обеспечению информационной безопасности страховой (перестраховочной) организации, требований к деятельности организаций по формированию и ведению базы данных, а также требованиями международных стандартов в области информационной безопасности и Правил обеспечения информационной безопасности информационных систем в АО «Банк ЦентрКредит» (далее – Банк).

5. Требования предъявляемые к процессам СУИБ Компании описанные в настоящей Политике, детально изложены во внутренних нормативных документах Компании, разработанных в соответствии с Главой 2 «Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной организации)» Постановления Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 30 июля 2018 года № 164 «Об утверждении Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной организации), а также кибербезопасности страховой (перестраховочной) организации», также Главами 5 и 6 «Формирование системы безопасности», «Минимальные требования к электронному оборудованию, сохранности базы данных и помещениям», Постановления Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 июля 2007 года № 177 «Об утверждении требований к деятельности организации по формированию и ведению базы данных).

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

6. 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.

7. К задачам СУИБ относятся:

1) категорирование информационных активов;

2) организация доступа к информационным системам;

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 системам;

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 действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на информационные активы Компании;

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 Компании;

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 Компании;

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

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 Компании, 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 Компании, непосредственно ориентированные на предоставление услуг клиентам, представляющие ценность для клиентов и обеспечивающих получение прибыли, определённых с процедурой, определяющей классификацию бизнес-процессов.

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

1) Индивидуальные устройства обработки информации;
2) Носители информации (в том числе на бумажном носителе);
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;
15) Информационные системы;
16) Интернет-ресурсы.

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

11. Доступ к информации и информационным системам предоставляется работникам в объеме, необходимом для исполнения их функциональных обязанностей.

12. В информационных системах используются только персонализированные пользовательские учетные записи пользователей.

13. Доступ к информационным системам осуществляется путем идентификации и аутентификации пользователей информационных систем. Идентификация и аутентификация пользователей информационных систем производится посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов многофакторной аутентификации.

14. Предоставление доступа к критичным информационным системам Компании производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей информационных систем их функциональным обязанностям.

15. 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.

16. Доступ лицам, не являющимся работниками Компании (далее – третьи лица) к информационным системам, предоставляется на период и в объеме, необходимом для проведения работ на основании соответствующего договора/соглашения содержащем требования по обеспечению информационной безопасности, за исключением случаев, предусмотренных законодательством Республики Казахстан. В договорах/соглашениях о соблюдении требований к информационной безопасности, заключаемых с третьими лицами, должны 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.

17. Компания применяет все необходимые организационные и технические меры, обеспечивающие эффективность процесса управления доступом к информационным системам.

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

18. Функции мониторинга по обеспечению информационной безопасности и мероприятия по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности Компании осуществляется работниками службы реагирования на инциденты информационной безопасности Банка (далее – Служба реагирования).

19. Служба реагирования и ответственный работник отдела информационной безопасности тесно взаимодействуют в целях обмена информацией о потенциальных угрозах, атаках, уязвимостях, участвуют в расследовании инцидентов информационной безопасности обеспечивая эффективную защиту информации Компании.

20. Служба реагирования обеспечивает:

1) подключение критичных информационных систем Компании к программно-техническим средствам по защиты информации Банка;

2) мониторинг событий информационной безопасности с применением систем мониторинга Банка в круглосуточном режиме, которые ведут сбор, анализ и корреляцию событии информационной безопасности;

3) сохранность и неизменность собранных данных (лог-файлов и других индикаторов компрометации, имеющих отношение к инциденту информационной безопасности не менее 5 лет);

4) разработку, поддержание в актуальном состоянии стандартных процедур реагирования и обучение работников Службы реагирования по вопросам применения стандартных процедур реагирования;

5) определение ответственных работников и (или) подразделений Банка, вовлеченных в процесс реагирования на инциденты информационной безопасности Компании;

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

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

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

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

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

11) 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.

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

21. Компания обеспечивает наличие документов, сведений и фактов, подтверждающих реализацию порядка реагирования на инциденты информационной безопасности Компании, а

также их консолидацию, систематизацию, целостность и сохранность информации об инцидентах информационной безопасности, результатах внутренних расследований инцидентов информационной безопасности и материалов расследований на бумажном носителе и (или) в электронном виде.

22. Срок хранения информации об инцидентах информационной безопасности, результатах внутреннего расследования инцидентов информационной безопасности и материалов расследования составляет не менее 5 (пяти) лет.

7. Требования к проведению анализа информации об инцидентах информационной безопасности

23. 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 отдел информационной безопасности обеспечивает:

1) проведение анализа выявленных инцидентов информационной безопасности Компании и нанесенного ими ущерба на рассмотрение Правлением Компании, 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 с учетом 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 Компании.

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

24. Участниками СУИБ Компании являются:

1) Совет директоров;
2) Правление;
3) Отдел информационных технологий;
4) Отдел информационной безопасности;
5) Отдел кадров;
6) Юридическая служба;
7) Служба комплаенса и ПОДиФТ;
8) Служба внутреннего аудита;
9) Отдел операционных рисков;
10) Бизнес-владельцы информационных систем;
11) Руководители структурных подразделений;
12) Работники структурных подразделений.

25. 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, и порядок работы с защищаемой информацией.

26. Правление утверждает внутренние нормативные документы по информационной безопасности, которые определяют правила и требования к обработке, хранению и передаче информации, а также меры по обеспечению защиты.

27. Правление для проверки знаний требований внутренних нормативных документов утверждает план проведения тестирования работников на знание требований внутренних нормативных документов по информационной безопасности, а также план проведения проверок на соответствие требованиям информационной безопасности.

28. Правление принимает решения по вопросам обеспечения информационной безопасности Компании и действует в рамках полномочий, предоставленных Советом Директоров.

29. Отдел информационных технологий осуществляет следующие функции:

1) разрабатывает и поддерживает в актуальном состоянии схемы информационной инфраструктуры, согласовывает их с Блоком информационных технологий Банка (далее – Блок ИТ);

2) разрабатывает и поддерживает в актуальном состоянии Приказы, внутренние нормативные документы по вопросам информационных технологий;

3) обеспечивает предоставление доступа пользователям к информационным системам Компании, за исключением специализированных информационных систем, доступ к которым предоставляется ИТ-владельцами информационных систем или Блоком ИТ;

4) обеспечивает конфигурирование системного и прикладного программного обеспечения Компании;

5) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Компании (включая резервирование и (или) архивирование и резервное копирование информации);

6) обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем;

7) обеспечивает установку обновлений безопасности на рабочие станции Компании;

8) взаимодействует с Блоком ИТ и отделом информационной безопасности в рамках функционирования СУИБ.

30. Отдел информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации осуществляет следующие функции:

1) разрабатывает Политику информационной безопасности Компании;

2) обеспечивает методологическую поддержку СУИБ Компании;

3) выстраивает СУИБ, осуществляет координацию и контроль деятельности подразделений Компании по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам участвует в расследовании инцидентов информационной безопасности Компании, при необходимости взаимодействует с работниками Центр обеспечения информационной безопасности Банка (далее – ЦОИБ);

4) участвует в организации процесса повышения осведомленности работников Компании в области информационной безопасности;

5) определяет перечень событий информационной безопасности, подлежащих мониторингу, источников таких событий, периодичности, порядка и методов мониторинга событий информационной безопасности;

6) определяет порядок отнесения событий информационной безопасности к инцидентам информационной безопасности, их классификации и приоритетности;

7) осуществляет оценку зрелости процессов СУИБ Компании;

8) проводит оценку рисков информационной безопасности;

9) подготавливает и предоставляет отчетность о реализации существенных рисков информационной безопасности в ЦОИБ, а также об устранении их последствий;

10) разрабатывает меры по обработке рисков информационной безопасности и предоставляет отчетность по их реализации в ЦОИБ;

11) определяет ограничения по использованию привилегированных учетных записей;

12) подготавливает предложения для принятия Правлением Компании решения по вопросам информационной безопасности;

13) информирует Председателя Правления о состоянии СУИБ в Компании;

14) собирает/анализирует материалы, необходимые для проведения внутреннего расследования инцидента информационной безопасности;

15) устанавливает причины возникновения инцидента информационной безопасности и порядок реализации инцидента информационной безопасности;

16) запрашивает у работников Компании предоставление пояснений (объяснительной) в письменном виде по выявленным фактам нарушений требований информационной безопасности;

17) оценивает масштаб воздействия и ущерб от реализации инцидента информационной безопасности;

18) оценивает эффективность принятых мер реагирования на расследуемый инцидент информационной безопасности;

19) подготавливает заключение 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;

20) проверяет права доступа работников Компании и третьих лиц к информационным активам Компании.

31. При отсутствии соответствующих средств защиты информации, потребности в экспертизе и невозможности проведения полноценного объективного расследования инцидента информационной безопасности, а также установления причин реализации инцидента информационной безопасности ответственный работник отдела информационной безопасности уполномочен привлекать работников ЦОИБ к расследованию инцидента информационной безопасности Компании.

32. Отдел обеспечения безопасности осуществляет следующие функции:

1) реализует комплекс мер физической и технической безопасности в Компании, в том числе организует пропускной и внутриобъектовый режим в центр обработки данных;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Компании (проводит инструктаж о неразглашении конфиденциальной информации);

3) контролирует внос/вынос/вывоз серверного и компьютерного оборудования Компании (согласно действующих процедур).

33. Отдел кадров осуществляет следующие функции:

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

2) организует мероприятия по повышению осведомленности работников Компании по вопросам информационной безопасности;

3) включает в трудовые договора/договора гражданско-правового характера/должностные инструкции/ положения о структурных подразделениях обязательства о соблюдении требовании по информационной безопасности.

34. Юридическая служба осуществляет:

1) правовую экспертизу внутренних нормативных документов Компании по вопросам обеспечения информационной безопасности;

2) консультирует/дает пояснения в части применения норм Законов Республики Казахстан по вопросам обеспечения информационной безопасности.

35. Служба комплаенса и ПОДиФТ совместно с Юридической службой определяет виды информации, подлежащие включению в перечень защищаемой информации, разрабатывают перечень и выносят на утверждение согласно пункта 24 настоящей Политики.

36. Служба внутреннего аудита проводит оценку состояния СУИБ Компании в соответствии с внутренними нормативными документами, регламентирующими организацию системы внутреннего аудита Компании (при необходимости привлекая работников ЦОИБ или

путем закупки услуги аудита информационной безопасности).

37. Отдел операционных рисков проводит анализ бизнес-процессов Компании на предмет выявления рисков информационной безопасности, выносит предложения по минимизации этих рисков.

38. Бизнес-владельцы информационных систем:

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;

3) согласовывают с отделом информационной безопасности вывод новых продуктов в боевую эксплуатацию, взаимодействуют на этапе разработки и запуска продуктов по вопросам обеспечения информационной безопасности.

39. Руководители структурных подразделений Компании:

1) обеспечивают ознакомление работников с внутренними нормативными документами Компании, содержащими требования к информационной безопасности;

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

40. Работники структурных подразделений Компании:

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

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) незамедлительно извещают своего непосредственного руководителя и ответственного работника отдела информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными системами.

41. Основные участники СУИБ со стороны Банка:

1) Блок ИТ;

2) ЦОИБ;

42. Блок ИТ осуществляет следующие функции:

1) рассматривает возможность/выделяет вычислительные мощности для ИТ-инфраструктуры Компании;

2) разворачивает и размещает в центах обработки данных Банка ИТ-инфраструктуру Компании, оказывает содействие ответственному работнику Отдела информационных технологий в разработке/актуализации схемы информационной инфраструктуры Компании, предоставляет актуальные данные, согласовывает разработанные схемы;

3) обеспечивает предоставление доступа пользователям Компании к информационным системам Компании, за исключением специализированных информационных систем, доступ к которым предоставляется ИТ-менеджерами информационных систем;

4) обеспечивает конфигурирование системного и прикладного программного обеспечения Компании;

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

6) устанавливает обновления безопасности и устраняет уязвимости на серверах.

43. ЦОИБ в целях обеспечения кураторства в построении взаимодействия между ЦОИБ и Компанией в части обеспечения необходимого и достаточного обеспечения уровня информационной безопасности осуществляет следующие функции по координации деятельности в области обеспечения информационной безопасности:

1) определяет требования по обеспечению информационной безопасности;

2) согласовывает внутренние нормативные документы в части информационной безопасности;

3) согласовывает предложения по внедрению организационных мер и программно-технических средств обеспечения информационной безопасности;

4) предоставляет, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;

5) согласовывает план мероприятий по реализации стратегии Компании в части обеспечения информационной безопасности;

6) определяет потребности в ресурсах, в том числе определение бюджета, связанного с реализацией мер, направленных на управление рисками информационной безопасности;

7) согласовывает требуемые мероприятий в области информационной безопасности с указанием сроков и ответственных исполнителей за их реализацию.

44. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Компании мер обеспечения информационной безопасности, при исполнении работником возложенных на него функциональных обязанностей, влечет за собой ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Компании.

9. Заключительные положения

45. Управляющий директор Компании/Ответственное лицо согласовывает с Правлением введение дополнительных мер контроля по частичной или полной остановке бизнес-процессов Компании, в случае получения информации от ответственного работника отдела информационной безопасности/или ЦОИБ о факте выявления инцидента информационной безопасности критичного уровня, не позволяющего продолжить штатную работу гарантировав при этом безопасность свойств информации – конфиденциальность, доступность и целостность.

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

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

48. 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.

49. Пересмотр / разработка настоящей Политики и нормативных документов Компании по вопросам обеспечения информационной безопасности осуществляет работник отдела информационной безопасности не реже одного раза в год.

Отдел информационной безопасности