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

2023 жылғы 30 қазандағы
№ 2023/21
Басқарма хаттамасымен
Мақұлданды

Директорлар кеңесі
сырттай отырысының
2023 жылғы 14 қарашадағы
№ 5-2023 хаттамасымен
Бекітілді

«Sinoasia B&R (Синоазия БиЭндАр) » СК» АҚ
Ақпараттық қауіпсіздік саясаты

1. Жалпы ережелер

1. Осы Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «СК «Sinoasia B&R (Синоазия БиЭндАр) » АҚ (бұдан әрі – Компания) ақпараттық қауіпсіздікті басқару жүйесінің (бұдан әрі – АҚБЖ) мақсаттарын, міндеттерін және іс-әрекет ету саласын айқындайтын Компанияның ақпараттық қауіпсіздікті басқару жүйесінің негізін қалайтын құжаты болып табылады.

2. Компания ақпараттық қауіпсіздікті қамтамасыз ету процесін басқаруға арналған Компанияның жалпы басқару жүйесінің бөлігі болып АҚБЖ құруды және оның қызмет етуін қамтамасыз етеді.

3. АҚБЖ Компанияның бизнес-процестеріне ықтимал залалдың ең төмен деңгейіне жол беретін Компанияның ақпараттық активтерін қорғауды қамтамасыз етеді.

4. Саясат Қазақстан Республикасының заңнамасына, соның ішінде сақтандыру (қайта сақтандыру) ұйымының ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, ұйымдардың деректер базасын қалыптастыру және жүргізу жөніндегі қызметіне қойылатын талаптарды реттейтін нормативтік құқықтық актілерге, сондай-ақ ақпараттық қауіпсіздік саласындағы халықаралық стандарттардың және «Centercredit банкі» АҚ (бұдан әрі – Банк) ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету ережелерінің талаптарына сәйкес әзірленген.

5. Осы Саясатта сипатталған Компанияның АҚБЖ процестеріне қойылатын талаптар Қазақстан Республикасы Қаржы нарығын және қаржы ұйымдарын реттеу мен қадағалау агенттігі Басқармасының 2018 жылғы 30 шілдедегі № 164 қаулысымен («Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптарды бекіту туралы») бекітілген «Сақтандыру (қайта сақтандыру) ұйымында сақталатын деректерге санкцияланбаған қол жеткізуден ақпараттың сақталуын және қорғалуын қамтамасыз ететін қауіпсіз жұмысты ұйымдастыруға, сондай-ақ сақтандыру (қайта сақтандыру) ұйымының киберқауіпсіздігіне қойылатын талаптардың» 2-тарауына, сондай-ақ Қазақстан Республикасы Қаржы нарығын және қаржы ұйымдарын реттеу мен қадағалау агенттігі Басқармасының 2007 жылғы 25 шілдедегі № 177 қаулысымен («Деректер базасын қалыптастыру және жүргізу жөніндегі ұйымның қызметіне қойылатын талаптарды бекіту туралы») бекітілген 5 және 6-тарауларына («Қауіпсіздік жүйесін қалыптастыру», «Электрондық жабдыққа, деректер базасының сақталуына және үй-жайларға қойылатын ең төменгі талаптар») сәйкес әзірленген Компанияның ішкі нормативтік құжаттарында егжей-тегжейлі баяндалған.

2. Ақпараттық қауіпсіздікті басқару жүйесін құрудың мақсаттары, міндеттері және негізгі приниптері

6. АҚБЖ мақсаты – ақпараттық қауіпсіздікті қамтамасыз ету процестерінің тиімділігін арттыру, ақпараттық активтердің құпиялылығының, тұтастығының және қолжетімділігінің талап

етілетін деңгейін қамтамасыз ету, соның салдарынан ақпараттық қауіпсіздік тәуекелдерін және олармен байланысты залалды азайту.

7. АҚБЖ міндеттеріне төмендегілер жатады:

1) ақпараттық активтерді санаттау;
2) ақпараттық жүйелерге қолжетімділікті ұйымдастыру;
3) ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету;
4) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметке және қатерлер мен осалдықтарды анықтау және талдау, шабуылдарға қарсы тұру және ақпараттық қауіпсіздік оқыс-оқиғаларын тергеу жөніндегі іс-шараларға мониторинг жүргізу;
5) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты, оған қоса ақпараттық жүйелердегі бұзылулар, іркілістер туралы мәліметтерді талдау;
6) ақпаратты криптографиялық қорғау құралдарын басқару тәртібін белгілеу;
7) үшінші тұлғалар ақпараттық жүйелерді пайдаланған кезінде ақпараттық қауіпсіздікті қамтамасыз ету;
8) ақпараттық қауіпсіздіктің жай-күйіне ішкі тексерулер жүргізу.

8. АҚБЖ құру және оның қызмет етуі келесі негізгі принциптерге сәйкес жүзеге асырылады:

1) заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын кез келген іс-әрекеттер қолданыстағы заңнаманың негізінде, заңнамада рұқсат етілген Компанияның ақпараттық активтеріне жағымсыз әсер ететін жағдайларды анықтау, олардың алдын алу, оқшаулау және жою әдістерін қолдану арқылы жүзеге асырылады;
2) бизнеске бағдарлану – ақпараттық қауіпсіздік Компанияның негізгі қызметін қолдау процесі ретінде қарастырылады, ақпараттық қауіпсіздікті қамтамасыз ету бойынша кез келген шаралар Компанияның бизнес-қызметін жүзеге асыруға мағызды кедергілер келтірмеуге тиіс;
3) кешенділік – ақпараттық активтердің бүкіл өмірлік циклі ішінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және барлық қызмет режимдерінде олардың қауіпсіздігін қамтамасыз ету;
4) негізділік және экономикалық мақсаттылық– пайдаланылатын мүмкіндіктер мен қорғаныс құралдары ғылым мен техниканың даму деңгейіне сәйкес іске асырылуға, қауіпсіздіктің берілген деңгейі тұрғысынан негізделуге және қойылатын талаптар мен нормаларға сәйкес келуге тиіс. Барлық жағдайда ақпараттық қауіпсіздікті қамтамасыз ету бойынша шаралар мен технологиялық шешімдердің құны Компанияның қорғалатын ақпараттық активтерінің құнынан аспауға тиіс;
5) бейімділік – ақпараттық активтердің маңыздылығына сәйкес ақпараттық активтерді қорғау әдістері мен құралдарын анықтау және қолдану;
6) қажетті білім мен артықшылықтардың төмен деңгейі – пайдаланушыға өз өкілеттіктері шегінде қызметтік міндеттерін орындауға қажетті ең аз артықшылықтар деңгейі беріледі және тек сол міндеттерді орындауға қажетті ақпараттық активтерге ғана қол жеткізуге рұқсат етіледі;
7) мамандану – ақпараттық қауіпсіздікті қамтамасыз ету бойынша шараларды іске асыру және технологиялық шешімдерді пайдалану кәсіби деңгейде дайындалған мамандармен жүзеге асырылуға тиіс;
8) ақпараттан хабардарлық және жеке жауапкершілік – барлық деңгейдегі басшылар мен орындаушылар ақпараттық қауіпсіздіктің барлық талаптарынан хабардар болуға және осы талаптардың орындалуы мен белгіленген ақпараттық қауіпсіздік шараларының сақталуына жеке жауапкершілік атқаруға тиіс;
9) өзара әрекеттесу және үйлестіру – ақпараттық қауіпсіздік бойынша шаралар Компанияның тиісті құрылымдық бөлімшелерінің өзара байланысы, қойылған мақсаттарға қол жеткізуге олардың күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен, кәсіби қауымдастықтармен және бірлестіктермен, мемлекеттік

органдармен, заңды және жеке тұлғалармен қажетті байланыстар орнату негізінде жүзеге асырылады;

10) растаушылық – ақпараттық қауіпсіздік талаптарының орындалуын және АҚБЖ тиімділігін растайтын дәлелдемелер жедел қолжеткізу және қалпына келтіру мүмкіндігімен жасалуға және сақталуға тиіс.

3. Ақпараттық қауіпсіздікті басқару жүйесінің әрекет ету саласы

9. АҚБЖ қолданыс аймағы болып клиенттерге қызметтер көрсетуге тікелей бағытталған, клиенттер үшін құндылығы бар және пайда алуды қамтамасыз ететін, бизнес-процестердің жіктеуішін айқындайтын процедурада белгіленген Компанияның негізгі бизнес-процестері танылады.

10. Қорғаныс объектілері негізгі бизнес-процестердің жұмыс істеуіне қажетті ақпараттық активтер болып табылады, оларға төмендегілер жатқызылуы мүмкін:

1) Ақпаратты өңдеудің жеке құрылғылары;
2) Ақпарат тасымалдағыштары (оның ішінде қағаз тасымалдағышы);
3) Перифериялық компьютерлік жабдық;
4) Серверлер;
5) Желілік жабдық;
6) Телефония аппаратурасы;
7) Физикалық байланыс арналары;
8) Деректер базалары;
9) Виртуалды байланыс арналары;
10) Виртуалдандыру жүйелері;
11) Операциялық жүйелер;
12) Аппараттық құрылғылардың бағдарламалық қамсыздандыруы;
13) Қолданбалы бағдарламалық қамсыздандыру;
14) Телефонияның бағдарламалық қамсыздандыруы;
15) Ақпараттық жүйелер;
16) Интернет-ресурстар.

4. Компанияның ақпараттық жүйелерінде құрылатын, сақталатын және өңделетін ақпаратқа қол жеткізуге қойылатын талаптар және ақпарат пен оның қолжетімділігіне мониторинг жүргізу

11. Ақпаратқа және ақпараттық жүйелерге қол жеткізу жұмыскерлерге олардың функционалдық міндеттерін орындауына қажетті көлемде ұсынылады.

12. Ақпараттық жүйелерде пайдаланушылардың тек дербестендірілген пайдаланушылық есептік жазбалары ғана қолданылады.

13. Ақпараттық жүйелерге қолжетімділік ақпараттық жүйелер пайдаланушыларын сәйкестендіру және аутентификациялау арқылы жүзеге асырылады. Ақпараттық жүйелер пайдаланушыларын сәйкестендіру және аутентификациялау «есептік жазба (сәйкестендіргіш) – құпиясөз» жұбын енгізу арқылы немесе көп факторлы аутентификация тәсілдерін қолдана отырып жүргізіледі.

14. Компанияның маңызды ақпараттық жүйелеріне қол жеткізу құқығы ақпараттық жүйелерді пайдаланушылардың рұқсат беру құқығының олардың қызметтік міндеттеріне сәйкестігін қамтамасыз етуге арналған рөлдерді қалыптастыру және енгізу арқылы беріледі

15. Технологиялық есептік жазбаларды пайдалануға оларды пайдалану және жаңартуына жеке жауап беретін тұлғаларды көрсете отырып, әрбір ақпараттық жүйеге арналған есептік жазбалардың тізбесіне сәйкес рұқсат беріледі.

16. Компания жұмыскерлері болып табылмайтын тұлғаларға (бұдан әрі – үшінші тұлғалар) ақпараттық жүйелерге қолжетімділік Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда, ақпараттық қауіпсіздікті қамтамасыз етуге қойылатын талаптарды қамтитын тиісті шарт/келісім негізінде жұмыстарды жүргізу үшін қажетті мерзімге және көлемде беріледі. Үшінші тұлғалармен жасалатын ақпараттық қауіпсіздік талаптарын сақтау туралы шарттарда/келісімдерде құпиялылық туралы ережелер, ақпараттық қауіпсіздікті бұзу, сондай-ақ үшінші тұлғалардың араласуынан туындаған ақпараттық жүйелер жұмысының іркілістері мен олардың қауіпсіздігінің бұзылуы салдарынан келтірілген залалды өтеу талаптары қамтылуға тиіс.

17. Компания ақпараттық жүйелерге қолжетімділікті басқару процесінің тиімділігін қамтамасыз ететін барлық қажетті ұйымдастырушылық және техникалық шараларды қолданады.

5. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтің және қауіпті анықтау мен талдау, шабуылдарға қарсы тұру және ақпараттық қауіпсіздік оқыс оқиғаларын тергеу бойынша іс-шаралардың мониторингін жүзеге асыруға қойылатын талаптар

18. Компанияның ақпараттық қауіпсіздікті қамтамасыз ету бойынша мониторинг функциялары мен қауіпті анықтау және талдау, шабуылдарға қарсы тұру және ақпараттық қауіпсіздік оқыс оқиғаларын тергеу бойынша іс-шараларды Банктің ақпараттық қауіпсіздік оқыс оқиғаларына ден қою қызметінің (бұдан әрі – Ден қою қызметі) жұмыскерлері жүзеге асырады.

19. Ден қою қызметі мен ақпараттық қауіпсіздік бөлімінің жауапты жұмыскері ықтимал қауіп-қатерлер, шабуылдар, осалдықтар туралы ақпарат алмасу мақсатында тығыз өзара іс-қимыл жасайды, Компания ақпаратының тиімді қорғалуын қамтамасыз ете отырып, ақпараттық қауіпсіздік оқыс оқиғаларын тергеуге қатысады.

20. Ден қою қызметі төмендегілерді қамтамасыз етеді:

1) Компанияның маңызды ақпараттық жүйелерін Банктің ақпаратты қорғау бойынша бағдарламалық-техникалық құралдарына қосуды;
2) ақпараттық қауіпсіздік оқиғаларын жинауды, талдауды және корреляциялауды жүргізетін Банктің мониторинг жүйелерін қолдана отырып, ақпараттық қауіпсіздік оқиғаларына тәулік бойы режимінде мониторинг жүргізуді;
3) жиналған деректердің сақталуы және өзгермеуі (ақпараттық қауіпсіздік инцидентіне қатысы бар лог-файлдар мен басқа да компрометация индикаторлары кемінде 5 жыл);
4) стандартты ден қою процедураларын әзірлеу, өзекті жай-күйінде ұстау және ден қою қызметінің жұмыскерлерін стандартты ден қою процедураларын қолдану мәселелері бойынша ақпараттық қауіпсіздіктің оқыс оқиғаларына қатысты оқытуды;
5) Компанияның ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесіне тартылған Банктің жауапты жұмыскерлерін және (немесе) бөлімшелерін анықтауды;
6) ақпараттық қауіпсіздіктің оқыс оқиғаларын жою бойынша кезек күттірмейтін шараларды қабылдау тәртібін анықтау, ақпараттық қауіпсіздіктің оқыс оқиғаларының туындау себептері мен салдарын анықтауды;
7) ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеу жүргізуіне қажетті материалдар жинауды және талдауды;
8) ақпараттық қауіпсіздіктің оқыс оқиғаларының туындау себептерін және ақпараттық қауіпсіздіктің оқыс оқиғаларын іске асыру тәртібін анықтауды;
9) ақпараттық қауіпсіздіктің оқыс оқиғаларын іске асуынан болған әсер ету ауқымы мен залалды бағалауды;
10) ақпараттық қауіпсіздіктің оқыс оқиғаларына қатысты тргеуге ден қою бойынша қабылданған шаралардың тиімділігін талдауды;
11) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат, сондай-ақ ақпараттық қауіпсіздіктің оқыс оқиғаларын қайта іске асудан болуы мүмкін залалды азайту мақсатында түзету шараларын қабылдау бойынша ұсынымдары көрсетілген

ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу нәтижелері туралы қорытынды әзірлеуді қамтамасыз етеді.

6. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауға, шоғырландыруға және сақтауға қойылатын талаптар

21. Компания Компанияның ақпараттық қауіпсіздік оқыс оқиғаларына ден қою тәртібінің іске асырылуын растайтын құжаттардың, мәліметтер мен фактілердің болуын, сондай-ақ ақпараттық қауіпсіздік оқыс оқиғалары, ақпараттық қауіпсіздіктің оқыс оқиғаларын ішкі тергеу нәтижелері туралы ақпараттың қағаз және (немесе) электрондық тасымалдағыштағы тергеу материалдарының шоғырландырылуын, жүйелендірілуін, тұтастығы мен сақталуын қамтамасыз етеді.

22. Ақпараттық қауіпсіздік оқыс оқиғалары, ақпараттық қауіпсіздікдің оқыс оқиғаларын ішкі тергеу нәтижелері туралы ақпаратты және тергеу материалдарын сақтау мерзімі кемінде 5 (бес) жылды құрайды.

7. Ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратқа талдауға қойылатын талаптар

23. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметке және ақпараттық қауіпсіздіктің оқыс оқиғалары бойынша қауіпті анықтау және талдау, шабуылдарға қарсы тұру және тергеу бойынша іс-шараларға мониторинг жүргізу процесінің тиімділігін арттыру мақсатында Ақпараттық қауіпсіздік бөлімі кемінде жылына бір рет:

1) ақпараттық қауіпсіздік тәуекелдерін бағалау, ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдарын түзету, бизнес-процестерді өзгерту мақсатында Компанияның анықталған ақпараттық қауіпсіздіктің оқыс оқиғаларына және олар келтірген залалға талдау жүргізуді Компания Басқармасының қарауына ұсынуды;
2) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің метрикаларын пайдалана отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесін түзету мақсатында тиімділікті бағалауды;
3) ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің тиімділігін бағалау нәтижесін ескере отырып, ақпараттық қауіпсіздіктің оқыс оқиғаларына ден қою процесінің метрикаларын қайта қарауды;
4) Компанияның мониторингке жататын ақпараттық қауіпсіздік оқиғаларының тізбесін, оқиғалар көздерін, мерзімділігін, ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу тәртібі мен әдістерін қайта қарауды қамтамасыз етеді.

8. Компанияның ақпараттық қауіпсіздікті қамтамасыз етуге жауапты жұмыскерлерінің жүктелген қызметтік міндеттерін орындаған кездегі жауапкершілігі

24. Компанияның АҚБЖ қатысушылары:

1) Директорлар кеңесі;
2) Басқарма;
3) Ақпараттық технологиялар бөлімі;
4) Ақпараттық қауіпсіздік бөлімі;
5) Кадрлар бөлімі;
6) Заң қызметі;
7) Комплаенс және қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл қызметі;
8) Ішкі аудит қызметі;
9) Операциялық тәуекелдер бөлімі;
10) Ақпараттық жүйелердің бизнес-иелері;
11) Құрылымдық бөлімшелердің басшылары;

12) Құрылымдық бөлімшелердің жұмыскерлері.

25. Директорлар кеңесі Ақпараттық қауіпсіздік саясатын және қорғалатын ақпараттың тізбесін, оның ішінде қызметтік, коммерциялық немесе заңмен қорғалатын өзге құпияны құрайтын мәліметтер туралы ақпаратты және қорғалатын ақпаратпен жұмыс істеу тәртібін бекітеді.

26. Басқарма ақпаратты өңдеу, сақтау және беру ережелері мен талаптарын, сондай-ақ қорғауды қамтамасыз ету шараларын айқындайтын ақпараттық қауіпсіздіктің ішкі нормативтік құжаттарын бекітеді.

27. Басқарма ақпараттық қауіпсіздікті басқару процесін реттейтін ішкі нормативтік құжаттарды, сонымен қатар ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне қатысты жұмыскерлердің хабардарлығын арттыру мақсатында жұмыскерлердің ақпараттық қауіпсіздік бойынша ішкі нормативтік құжаттардың талаптарын білуіне тестілеу жүргізу жоспарын бекітеді.

28. Басқарма Компанияның ақпараттық қауіпсіздігін қамтамасыз ету мәселелері бойынша шешімдер қабылдайды және Директорлар кеңесі берген өкілеттіктер шеңберінде әрекет етеді.

29. Ақпараттық технологиялар бөлімі келесі функцияларды жүзеге асырады:

1) ақпараттық инфрақұрылым схемаларын әзірлейді және олардың өзектілігін қамтамасыз етеді, Банктің ақпараттық технологиялар блогымен (бұдан әрі – АТ блогы) келіседі;
2) ақпараттық технологиялар мәселелері бойынша бұйрықтарды, ішкі нормативтік құжаттарды әзірлейді және олардың өзектілігін қамтамасыз етеді;
3) ақпараттық жүйелердің АТ-иелері немесе АТ блогы қолжетімділік беретін мамандандырылған ақпараттық жүйелерді қоспағанда, пайдаланушыларға Компанияның ақпараттық жүйелеріне қолжетімділік берілуін қамтамасыз етеді;
4) Компанияның жүйелік және қолданбалы бағдарламалық қамсыздандырудың конфигурациясын қамтамасыз етеді;
5) ақпараттық инфрақұрылымның үздіксіз жұмыс істеуіне, Компанияның ақпараттық жүйелеріндегі деректердің құпиялылығына, тұтастығына және қолжетімділігіне қойылатын белгіленген талаптардың орындалуын қамтамасыз етеді (оның ішінде ақпаратты резервтеу және (немесе) архивтеу және резервтік көшірмесін жасау);
6) ақпараттық жүйелерді таңдау, енгізу, әзірлеу және тестілеу кезінде ақпараттық қауіпсіздік талаптарының сақталуын қамтамасыз етеді;
7) Компанияның жұмыс станцияларына қауіпсіздік жаңартуларының орнатылуын қамтамасыз етеді;
8) АҚБЖ қызмет істеу шеңберінде АТ блогымен және ақпараттық қауіпсіздік бөлімімен өзара іс-қимыл жасайды.

30. Ақпараттық қауіпсіздік бөлімі ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету мақсатында келесі функцияларды жүзеге асырады:

1) Компанияның Ақпараттық қауіпсіздік саясатын әзірлейді;
2) Компания АҚБЖ әдіснамалық қолдауды қамтамасыз етеді;
3) АҚБЖ құрады, Компанияның құрылымдық бөлімшелерінің ақпараттық қауіпсіздікті қамтамасыз ету, қауіптерді анықтау және талдау, шабуылдарға қарсы іұру бойынша қызметін үйлестіреді және бақылайды, Компанияның ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеуге қатысады, қажет болған жағдайда Банктің Ақпараттық қауіпсіздікті қамтамасыз ету орталығының (бұдан әрі – АҚҚО) жұмыскрлерімен өзара әрекеттеседі.
4) Компания жұмыскерлерінің ақпараттық қауіпсіздік саласындағы хабардарлығын арттыру процесін ұйымдастыруға қатысады;
5) мониторингке жататын ақпараттық қауіпсіздік оқиғаларының тізбесін, осындай оқиғалардың көздерін, мерзімділігін, ақпараттық қауіпсіздік оқиғаларына мониторинг жүргізу тәртібі мен әдістерін айқындайды;

6) ақпараттық қауіпсіздік оқиғаларын ақпараттық қауіпсіздіктің оқыс оқиғаларына жатқызу тәртібін, олардың жіктелуін және басымдылығын айқындайды;
7) Компания АҚБЖ процестерінің жетілу деңгейін бағалауды жүзеге асырады;
8) ақпараттық қауіпсіздік тәуекелдеріне бағалау жүргізеді;
9) ақпараттық қауіпсіздіктің елеулі тәуекелдерінің іске асуы және олардың салдарларын жою туралы есептілікті дайындайды және АҚҚО ұсынады;
10) ақпараттық қауіпсіздік тәуекелдерін өңдеу шараларын әзірлейді және олардың іске асу есептілігін АҚҚО ұсынады;
11) артықшылықты есептік жазбаларды пайдалануға шектеулерді айқындайды;
12) ақпараттық қауіпсіздік мәселелері бойынша Компанияның Басқармасы шешім қабылдауы үшін ұсыныстар дайындайды;
13) Басқарма Төрағасына Компаниядағы АҚБЖ жай-күйі туралы хабарлайды;
14) ақпараттық қауіпсіздіктің оқыс оқиғаларына ішкі тергеу жүргізуге қажетті материалдарды жинайды/талдайды;
15) ақпараттық қауіпсіздіктің оқыс оқиғаларын туындау себептерін және ақпараттық қауіпсіздік оқыс оқиғаларының жүзеге асу тәртібін анықтайды;
16) Компания жұмыскерлерінен ақпараттық қауіпсіздік талаптарын бұзудың анықталған фактілері бойынша жазбаша түрде түсініктеме (түсіндірме хат) ұсынуды сұратады;
17) ақпараттық қауіпсіздік оқыс оқиғаларының іске асуынан болған әсер ету масштабы мен залалды бағалайды;
18) ақпараттық қауіпсіздіктің тергелетін оқыс оқиғаларына ден қою шараларының тиімділігін бағалайды;
19) ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпарат, сондай-ақ ақпараттық қауіпсіздіктің оқыс оқиғаларын қайта іске асудан болуы мүмкін залалды азайту мақсатында түзету шараларын қабылдау бойынша ұсынымдары көрсетілген ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу нәтижелері туралы қорытынды дайындайды.
20) Компания жұмыскерлерінің және үшінші тұлғалардың Компанияның ақпараттық активтеріне қолжетімділік құқықтарын тексереді.

31. Ақпаратты қорғаудың тиісті құралдары болмаған, сараптама қажеттілігі туындаған және ақпараттық қауіпсіздіктің оқыс оқиғасына толыққанды объективті тергеп-тексеру жүргізу, сондай-ақ ақпараттық қауіпсіздік оқыс оқиғаларының іске асу себептерін анықтау мүмкін болмаған кезде ақпараттық қауіпсіздік бөлімінің жауапты жұмыскері АҚҚО жұмыскерлерін Компанияның ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеп-тексеруге тартуға уәкілетті.

32. Қауіпсіздікті қамтамасыз ету бөлімі келесі функцияларды жүзеге асырады:
1) Компаниядағы физикалық және техникалық қауіпсіздік шараларының кешенін іске асырады, оның ішінде деректерді өңдеу орталығына рұқсатнама арқылы өткізу және объектішілік режимді ұйымдастырады;
2) Компания жұмыскерлерін жұмысқа қабылдау және жұмыстан босату кезінде ақпараттық қауіпсіздік қатерлерінің туындау тәуекелдерін барынша азайтуға бағытталған профилактикалық іс-шараларды жүргізеді (құпия ақпаратты жария етпеу туралы нұсқама жүргізеді);
3) Компанияның серверлік және компьютерлік жабдығын әкелуді/әкетуді/шығаруды (қолданыстағы процедураларға сәйкес) бақылайды.

33. Кадрлар бөлімі келесі функцияларды жүзеге асырады:
1) Компания жұмыскерлерінің, сондай-ақ қызметтер көрсету туралы шарт бойынша жұмысқа тартылған тұлғалардың, тағылымдамадан өтушілердің, практиканттардың құпия ақпаратты жария етпеу туралы міндеттемелерге қол қоюын қамтамасыз етеді;
2) Компания жұмыскерлерінің ақпараттық қауіпсіздік мәселелері бойынша хабардарлығын арттыру бойынша іс-шараларды ұйымдастырады;

3) еңбек шарттарына/азаматтық-құқықтық сипаттағы шарттарға/лауазымдық нұсқаулықтарға/құрылымдық бөлімшелер туралы ережелерге ақпараттық қауіпсіздік бойынша талаптарды сақтау туралы міндеттемелерді енгізеді.

34. Заң қызметі төмендегілерді жүзеге асырады:

1) ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша Компанияның ішкі нормативтік құжаттарына құқықтық сараптама жүргізеді;

2) ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша Қазақстан Республикасы Заңдарының нормаларын қолдану бөлігінде кеңес /түсініктеме береді.

35. Комплаенс және қылмыстық жолмен алынған кірістерді заңдастыруға (жылыстатуға) және терроризмді қаржыландыруға қарсы іс-қимыл қызметі Заң қызметімен бірлесіп қорғалатын ақпараттың тізбесіне енгізуге жататын ақпарат түрлерін айқындайды, тізбені әзірлейді және осы Саясаттың 24-тармағына сәйкес бекітуге шығарады.

36. Ішкі аудит қызметі Компанияның ішкі аудит жүйесін ұйымдастыруды реттейтін ішкі нормативтік құжаттарына сәйкес Компанияның АҚБЖ жай-күйіне бағалау жүргізеді (қажет болған кезде АҚҚО жұмыскерлерін тарта отырып немесе ақпараттық қауіпсіздік аудитінің қызметін сатып алу арқылы).

37. Операциялық тәуекелдер бөлімі ақпараттық қауіпсіздік тәуекелдерін анықтау мақсатында Компанияның бизнес-процестеріне талдау жүргізеді, осы тәуекелдерді барынша азайту жөнінде ұсыныстар енгізеді.

38. Ақпараттық жүйелердің бизнес-иелері:

1) Қызметтер мен өнімдерді құрған, енгізген, модификациялаған, клиенттерге ұсынған кезде ақпараттық қауіпсіздікке қойылатын талаптардың сақталуына жауап береді;

2) Ақпараттық жүйелерге кіруге рұқсат беретін матрицаларды құрады және олардың актуалды болуына қолдау көрсетеді.

3) жаңа өнімдерді өнеркәсіптік пайдалануға енгізуді ақпараттық қауіпсіздік бөлімімен келіседі, өнімдерді әзірлеу және іске қосу кезеңінде ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша өзара әрекеттеседі.

39. Компанияның құрылымдық бөлімшелерінің басшылары:

1) жұмыскерлердің ақпараттық қауіпсіздікке қойылатын талаптар қамтылатын Компанияның ішкі нормативтік құжаттарымен танысуын қамтамасыз етеді;

2) өздері басқаратын бөлімшелерде ақпараттық қауіпсіздікті қамтамасыз ету үшін жеке жауапкершілік көтереді.

40. Компанияның құрылымдық бөлімшелерінің жұмыскерлері:

1) Компанияда қабылданған ақпараттық қауіпсіздікке қойылатын талаптарының сақталуына жауап береді;

2) Өзінің қызметтік міндеттемелері аясында бірлесіп әрекет ететін үшінші тұлғалардың

3) ақпараттық қауіпсіздікке қойылатын талаптарды орындауын, соның ішінде аталған талаптарды үшінші тұлғалармен жасалатын шарттарға қосу арқылы бақылайды;

4) ақпараттық жүйелермен жұмыс кезіндегі барлық күмәнді жағдайлар мен бұзушылықтар туралы өзінің тікелей басшысына және ақпараттық қауіпсіздік бөлімінің жауапты жұмыскеріне дереу хабарлайды.

41. Банк тарапынан АҚБЖ негізгі қатысушылары:

1) АТ блогы;

2) АҚҚО.

42. АТ блогы келесі функцияларды жүзеге асырады:

1) Компанияның АТ-инфрақұрылымы үшін есептеу қуаттарын бөлу мүмкіндігін қарайды/бөледі;

2) Компанияның АТ-инфрақұрылымын Банктің деректерді өңдеу орталықтарында орналастырады және орналасуын қамтамасыз етеді, Ақпараттық технологиялар бөлімінің жауапты жұмыскеріне Компанияның ақпараттық инфрақұрылым сұлбасын

әзірлеуде/өзектілендіруде жәрдемдеседі, өзекті деректерді ұсынады, әзірленген схемаларды келістіреді;

3) қолжетімділігі ақпараттық жүйелердің АТ-менеджерлері арқылы берілетін мамандандырылған ақпараттық жүйелерді қоспағанда, өздерінің функционалдық міндеттері шеңберінде Компания пайдаланушыларына Компанияның ақпараттық жүйелеріне қолжетімділік беруді қамтамасыз етеді;
4) Компанияның жүйелік және қолданбалы бағдарламалық жасақтама конфигурациясын қамтамасыз етеді;
5) ішкі SLA сәйкес ақпараттық инфрақұрылымның жұмыс істеуінің үздіксіздігі, ақпараттық жүйелер деректерінің құпиялылығы, тұтастығы және қолжетімділігі бойынша белгіленген талаптардың орындалуын (ақпаратты резервтеуді және (немесе) архивтеуді және резервтік көшіруді қоса алғанда) қамтамасыз етеді;
6) серверлерде қауіпсіздік жаңартуларын орнатады және осалдықтарды жояды.

43. Ақпараттық қауіпсіздіктің қажетті және жеткілікті деңгейін қамтамасыз ету бөлігінде АҚҚО мен Компания арасындағы өзара іс-қимылды ұйымдастыруға жетекшілік ету мақсатында АҚҚО ақпараттық қауіпсіздікті қамтамасыз ету саласындағы қызметті үйлестіру бойынша төмендегі функцияларды жүзеге асырады:

1) ақпараттық қауіпсіздікті қамтамасыз ету бойынша талаптарды айқындайды;
2) ақпараттық қауіпсіздік бөлігінде ішкі нормативтік құжаттарды келісуге шығарады;
3) ұйымдастырушылық шараларды және бағдарламалық-техникалық құралдарды енгізу бойынша ұсыныстарды келісімге ұсынады;
4) ақпараттық қауіпсіздікті қамтамасыз ету процесін автоматтандыратын бағдарламалық-техникалық құралдардың тиісінше жұмыс істеуін, сондай-ақ оларға қол жеткізуді қамтамасыз етеді;
5) Компания стратегиясын ақпараттық қауіпсіздікті қамтамасыз ету бөлігінде іске асыру жөніндегі іс-шаралар жоспарын келісімге алады;
6) ресурстарға қажеттілікті, оның ішінде ақпараттық қауіпсіздік тәуекелдерін басқаруға бағытталған шараларды іске асырумен байланысты бюджетті айқындауды анықтайды;
7) ақпараттық қауіпсіздік саласындағы талап етілетін іс-шараларды олардың мерзімдері мен іске асыруға жауапты орындаушылары көрсетіле отырып келісімге ұсынылады.

44. Жұмыскер өзіне жүктелген қызметтік міндеттемелерді орындаған кезде, ақпараттық ресурстарды пайдалану тәртібі мен ережесін және ақпараттық қауіпсіздікті қамтамасыз ету бойынша Компанияда қабылданған шараларды сақтамауы Қазақстан Республикасының қолданыстағы заңнамасына және Компанияның ішкі нормативтік құжаттарына сәйкес жауапкершілікке әкеледі.

9. Қорытынды ережелер

45. Компанияның Басқарушы директоры/Жауапты тұлға ақпараттық қауіпсіздіктің маңызды деңгейдегі оқыс оқиғасы анықталған фактісі туралы ақпарат алған жағдайда, ақпарат қасиеттерінің – құпиялылықтың, қолжетімділіктің және тұтастықтың қауіпсіздігіне кепілдік бере отырып, штаттық жұмысты жалғастыруға мүмкіндік бермейтін ақпараттық қауіпсіздік бөлімінің жауапты жұмыскерінен/немесе АҚҚО Компанияның бизнес-процестерін ішінара немесе толық тоқтату бойынша қосымша бақылау шараларын енгізуді Басқармамен келіседі.

46. Осы Саясатпен реттелмеген барлық мәселелер Қазақстан Республикасының заңнамасына, ішкі нормативтік құжаттарға және Компанияның уәкілетті органдарының шешімдеріне, сондай-ақ Компания қызметінің қалыптасқан практикасына сәйкес шешіледі.

47. Саясат Директорлар кеңесі бекіткен күннен бастап күшіне енеді және Директорлар кеңесі оны күші жойылды деп таныған кезден бастап өз қолданысын тоқтатады.

48. Қазақстан Республикасы заңнамасының өзгеруі нәтижесінде осы Саясаттың жекелеген нормалары Қазақстан Республикасының қолданыстағы заңнамасына қайшы келген жағдайда, Саясатқа өзгерістер енгізілгенге дейін Қазақстан Республикасының қолданыстағы заңнамасын және Қазақстан Республикасының заңнамасына қайшы келмейтін бөлігіндегі Саясатты басшылыққа алу қажет.

49. Осы Саясатты және Компанияның ақпараттық қауіпсіздік мәселелері бойынша нормативтік құжаттарын қайта қарауды/әзірлеуді ақпараттық қауіпсіздік бөлімінің жұмыскері жылына кемінде бір рет жүзеге асырады.

Ақпараттық қауіпсіздік бөлімі

Endorsed pursuant to
Management Board Minutes
No. 2023/21 dated 30.10.2023.

Approved pursuant to
Minutes No. 5-2023 of the Board of
Directors' meeting held by absentee
voting, dated 14.11.2023.

[Signature]
[Seal: Republic of Kazakhstan; "Sinoasia B&R Insurance" JSC; "Sinoasia B&R"; BIN 071240007099]

Information Security Policy of "Sinoasia B&R Insurance" JSC

1. General Provisions

1. This Information Security Policy (the Policy) is the foundational document of the information security management system of "Sinoasia B&R Insurance" JSC (the Company) and defines the objectives, tasks, and scope of the Company's information security management system (ISMS).

2. The Company ensures the establishment, operation, and development of the ISMS, which forms part of the Company's overall management system and is designed to manage information security processes.

3. The ISMS protects the Company's information assets to keep potential damage to the Company's business processes to a minimum.

4. The Policy has been developed in accordance with the laws of the Republic of Kazakhstan, including regulatory legal acts governing information security requirements for insurance (reinsurance) organizations and requirements for the activities of organizations that establish and maintain databases, as well as the requirements of international information security standards and the Rules to Ensure the Information Security of Information Systems at Bank CenterCredit JSC (the Bank).

5. The Company's internal regulatory documents set out in detail the requirements for the Company's ISMS processes described in this Policy. These documents have been developed in accordance with Chapter 2 of the Requirements for Secure Operations to Safeguard Information and Protect Data Held by an Insurance (Reinsurance) Organization Against Unauthorized Access, and to Ensure the Cybersecurity of an Insurance (Reinsurance) Organization, approved by Resolution No. 164 of the Management Board of the Agency of the Republic of Kazakhstan for Regulation and Supervision of the Financial Market and Financial Organizations dated July 30, 2018, "On Approval of the Requirements for Secure Operations to Safeguard Information and Protect Data Held by an Insurance (Reinsurance) Organization Against Unauthorized Access, and to Ensure the Cybersecurity of an Insurance (Reinsurance) Organization," and Chapters 5 and 6, "Establishment of a Security System" and "Minimum Requirements for Electronic Equipment, Database Safeguards, and Premises," respectively, of the requirements approved by Resolution No. 177 of the Management Board of the Agency of the Republic of Kazakhstan for Regulation and Supervision of the Financial Market and Financial Organizations dated July 25, 2007, "On Approval of Requirements for the Activities of an Organization That Establishes and Maintains a Database."

2. Objectives, Tasks, and Core Principles to Establish an Information Security Management System

6. The ISMS aims to improve the effectiveness of information security processes and ensure the required levels of confidentiality, integrity, and availability of information assets, thereby reducing information security risks and the resulting damage.

7. The tasks of the ISMS include:

1) categorizing information assets;

2) managing access to information systems;

3) ensuring the security of the information infrastructure;

4) monitoring information security activities and measures to identify and analyze threats and vulnerabilities, counter attacks, and investigate information security incidents;

5) analyzing information on information security incidents, including details of violations and information system failures;

6) defining the procedure to manage cryptographic information protection tools;

7) ensuring information security when third parties access information systems;

8) conducting internal information security reviews.

8. The establishment and operation of the ISMS are governed by the following core principles:

1) legality: all actions to ensure information security must comply with applicable laws and use all legally permitted methods to detect, prevent, contain, and stop adverse effects on the Company's information assets;

2) business alignment: information security is a process that supports core business activities, and information security measures must not create significant obstacles to the Company's business operations;

3) comprehensiveness: information assets must remain secure throughout their life cycle, at every technological stage of their use, and in every operating mode;

4) justification and economic feasibility: the protection capabilities and tools used must reflect the appropriate level of scientific and technological development, be justified in terms of the specified security level, and comply with applicable requirements and standards. The cost of information security measures and technological solutions must never exceed the value of the Company's information assets they protect;

5) adaptability: the methods and tools to protect information assets must be selected and applied according to the criticality of those assets;

6) need to know and least privilege: users receive the minimum privileges and access only to the information assets they need to perform their duties within the scope of their authority;

7) specialization: professionally trained specialists must implement information security measures and operate information security technologies;

8) awareness and personal responsibility: managers at all levels and staff members must be aware of all information security requirements and are personally responsible for compliance with those requirements and established information security measures;

9) cooperation and coordination: information security measures must be implemented through cooperation among the Company's relevant organizational units, coordination of their efforts to achieve established objectives, and the establishment of necessary relationships with external organizations, professional associations and communities, government authorities, legal entities, and individuals;

10) verifiability: evidence of compliance with information security requirements and of ISMS effectiveness must be created and retained in a form that allows prompt access and recovery.

3. Scope of the Information Security Management System

9. The ISMS covers the Company's core business processes that directly support the provision of services to customers, deliver value to customers, and generate profit, as identified in accordance with the procedure that classifies business processes.

10. The assets to be protected are information assets required to operate core business processes and may include:

1) Individual data processing devices;
2) Information storage media, including paper media;
3) Computer peripherals;
4) Servers;
5) Network equipment;
6) Telephony equipment;
7) Physical communication channels;
8) Databases;
9) Virtual communication channels;
10) Virtualization systems;
11) Operating systems;
12) Software for hardware devices;
13) Application software;
14) Telephony software;
15) Information systems;
16) Internet resources.

4. Requirements Governing Access to Information Created, Stored, and Processed in the Company's Information Systems and the Monitoring of Such Information and Access to It

11. Employees are granted access to information and information systems to the extent necessary to perform their duties.

12. Information systems must use only user accounts assigned to individual users.

13. Users must be identified and authenticated to access information systems. Information system users are identified and authenticated by entering an account identifier and password or through multifactor authentication methods.

14. Access to the Company's critical information systems is granted through the definition and implementation of roles to ensure that users' access rights correspond to their duties.

15. Service accounts may be used only in accordance with a list of such accounts for each information system that identifies the individuals personally responsible for their use and required to keep them up to date.

16. Individuals who are not Company employees (third parties) are granted access to information systems for the period and to the extent necessary to perform work under an appropriate contract/agreement that includes information security requirements, except as provided by the laws of the Republic of Kazakhstan. Contracts/agreements with third parties on compliance with information security requirements must include confidentiality provisions and terms governing compensation for damage caused by information security breaches and by information system failures and security breaches resulting from third-party interference.

17. The Company implements all necessary organizational and technical measures to ensure the effectiveness of the process to manage access to information systems.

5. Requirements to Monitor Information Security Activities and Measures to Identify and Analyze Threats, Counter Attacks, and Investigate Information Security Incidents

18. Employees of the Bank's Information Security Incident Response Service (the Incident Response Service) monitor the Company's information security activities and implement measures to identify and analyze threats, counter attacks, and investigate information security incidents.

19. The Incident Response Service and the responsible employee of the Information Security Department work closely together to exchange information on potential threats, attacks, and vulnerabilities and participate in information security incident investigations to ensure the effective protection of the Company's information.

20. The Incident Response Service must:

1) connect the Company's critical information systems to the Bank's information protection hardware and software tools;

2) monitor information security events around the clock through the Bank's monitoring systems, which collect, analyze, and correlate information security events;

3) retain and preserve without alteration the collected data, including log files and other indicators of compromise related to an information security incident, for at least 5 years;

4) develop and maintain up-to-date standard response procedures and train Incident Response Service employees to apply those procedures;

5) identify the responsible employees and/or units of the Bank involved in the response to the Company's information security incidents;

6) define the procedure to take urgent measures to resolve information security incidents and determine their causes and consequences;

7) collect and analyze materials required to conduct an internal information security incident investigation;

8) determine the causes of an information security incident and the sequence of events through which it occurred;

9) assess the extent of the impact and damage caused by an information security incident;

10) analyze the effectiveness of the response measures taken to address the information security incident under investigation;

11) prepare a report on the findings of the information security incident investigation that includes details of the incident and recommendations on corrective measures to reduce the likelihood of recurrence and the potential damage.

6. Requirements to Collect, Consolidate, and Retain Information on Information Security Incidents

21. The Company ensures the availability of documents, records, and evidence confirming the implementation of its information security incident response procedure. The Company also ensures the consolidation, systematic organization, integrity, and safekeeping of such documentation, information on information security incidents and the results of internal incident investigations, and investigation materials, in paper and/or electronic form.

22. Information on information security incidents, the results of internal information security incident investigations, and investigation materials must be retained for at least 5 (five) years.

7. Requirements to Analyze Information on Information Security Incidents

23. The Information Security Department must perform the following at least once a year to improve the effectiveness of the process to monitor information security activities and measures to identify and analyze threats, counter attacks, and investigate information security incidents:

1) analyze the Company's identified information security incidents and the damage they caused and submit the results to the Company's Management Board for consideration to assess information security risks, adjust information security methods and tools, and modify business processes;

2) assess the effectiveness of the information security incident response process through its metrics to adjust the process;

3) review the information security incident response process metrics in light of the results of the process effectiveness assessment;

4) review the list of information security events to be monitored, the event sources, and the frequency, procedures, and methods to monitor the Company's information security events.

8. Company Employees' Responsibility to Ensure Information Security in the Performance of Their Assigned Duties

24. The participants in the Company's ISMS are:

1) The Board of Directors;
2) The Management Board;
3) The Information Technology Department;
4) The Information Security Department;
5) The Human Resources Department;
6) The Legal Service;
7) The Compliance and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Service;
8) The Internal Audit Service;
9) The Operational Risk Department;
10) Information system business owners;
11) Heads of organizational units;
12) Employees of organizational units.

25. The Board of Directors approves the Information Security Policy, the list of protected information, including official secrets, trade secrets, and other legally protected confidential information, and the procedure to handle protected information.

26. The Management Board approves internal information security regulatory documents that establish rules and requirements governing the processing, storage, and transmission of information, as well as protective measures.

27. The Management Board approves a plan to test employees' knowledge of the requirements set out in internal information security regulatory documents, as well as a plan to conduct information security compliance reviews.

28. The Management Board makes decisions on the Company's information security matters and acts within the authority granted by the Board of Directors.

29. The Information Technology Department performs the following functions:

1) develops and maintains up-to-date information infrastructure diagrams and obtains endorsement of them from the Bank's Information Technology Division (the IT Division);

2) develops and maintains up-to-date orders and internal regulatory documents on information technology matters;

3) ensures that users are granted access to the Company's information systems, except for specialized information systems to which access is granted by the information systems' IT owners or the IT Division;

4) ensures the configuration of the Company's system and application software;

5) ensures compliance with the established requirements for the continuity of information infrastructure operations and the confidentiality, integrity, and availability of data in the Company's information systems, including redundancy and/or archiving and information backups;

6) ensures compliance with information security requirements during the selection, implementation, development, and testing of information systems;

7) ensures that security updates are installed on the Company's workstations;

8) cooperates with the IT Division and the Information Security Department as part of ISMS operations.

30. The Information Security Department performs the following functions to ensure the confidentiality, integrity, and availability of information:

1) develops the Company's Information Security Policy;

2) provides methodological support for the Company's ISMS;

3) establishes the ISMS, coordinates and oversees the Company's organizational units' information security activities and measures to identify and analyze threats and counter attacks, participates in the investigation of the Company's information security incidents, and cooperates with employees of the Bank's Information Security Center (ISC) as necessary;

4) participates in organizing the process to raise Company employees' information security awareness;

5) defines the list of information security events to be monitored, the sources of such events, and the frequency, procedures, and methods to monitor information security events;

6) defines the procedure to designate information security events as information security incidents and to classify and prioritize those incidents;

7) assesses the maturity of the Company's ISMS processes;

8) assesses information security risks;

9) prepares and submits reports to the ISC on material information security risk events and the remediation of their consequences;

10) develops information security risk treatment measures and reports on their implementation to the ISC;

11) defines restrictions on the use of privileged accounts;

12) prepares proposals to support the Company's Management Board in its decisions on information security matters;

13) informs the Chair of the Management Board of the status of the Company's ISMS;

14) collects and analyzes materials required to conduct an internal information security incident investigation;

15) determines the causes of an information security incident and the sequence of events through which it occurred;

16) requests written explanations (explanatory statements) from Company employees concerning identified violations of information security requirements;

17) assesses the extent of the impact and damage caused by an information security incident;

18) assesses the effectiveness of the response measures taken to address the information security incident under investigation;

19) prepares a report on the findings of the information security incident investigation that includes details of the incident and recommendations on corrective measures to reduce the likelihood of recurrence and the potential damage;

20) reviews Company employees' and third parties' access rights to the Company's information assets.

31. The responsible employee of the Information Security Department is authorized to involve ISC employees in the investigation of a Company information security incident when appropriate information protection tools are unavailable, expert assistance is required, and a comprehensive, objective investigation and determination of the incident's causes cannot be completed.

32. The Security Department performs the following functions:

1) implements a range of physical and technical security measures within the Company, including access controls and internal security arrangements for the data center;

2) takes preventive measures to minimize the risk of information security threats arising when Company employees are hired or their employment is terminated, including briefings on the nondisclosure of confidential information;

3) controls the movement of the Company's server and computer equipment into and out of the premises, including its removal by vehicle, in accordance with applicable procedures.

33. The Human Resources Department performs the following functions:

1) ensures that Company employees, individuals engaged under service agreements, trainees, and interns sign confidentiality undertakings;

2) organizes activities to raise Company employees' information security awareness;

3) includes obligations to comply with information security requirements in employment contracts, civil law contracts, job descriptions, and organizational unit regulations.

34. The Legal Service performs the following functions:

1) conducts legal reviews of the Company's internal regulatory documents on information security matters;

2) provides advice and explanations on the application of the laws of the Republic of Kazakhstan to information security matters.

35. The Compliance and AML/CFT Service and the Legal Service jointly identify the types of information to be included in the list of protected information, develop the list, and submit it for approval in accordance with paragraph 24 of this Policy.

36. The Internal Audit Service assesses the status of the Company's ISMS in accordance with the internal regulatory documents governing the Company's internal audit system, involving ISC employees or procuring information security audit services as necessary.

37. The Operational Risk Department analyzes the Company's business processes to identify information security risks and submits proposals to minimize those risks.

38. Information system business owners:

1) are responsible for compliance with information security requirements when products and services are created, implemented, modified, and provided to customers;

2) develop and maintain up-to-date information system access matrices;

3) obtain the Information Security Department's endorsement to launch new products in the production environment and cooperate on information security matters during product development and launch.

39. Heads of the Company's organizational units:

1) ensure that employees familiarize themselves with the Company's internal regulatory documents that contain information security requirements;

2) are personally responsible for information security
in the units they head.

40. Employees of the Company's organizational units:

1) are responsible for compliance with the Company's information security requirements;

2) oversee compliance with information security requirements by third parties with whom they interact in the performance of their duties, including by incorporating those requirements into contracts with third parties;

3) immediately notify their direct supervisor and the responsible employee of the Information Security Department of all suspicious situations and violations encountered when using information systems.

41. The principal participants in the ISMS on the Bank's side are:

1) The IT Division;

2) The ISC.

42. The IT Division performs the following functions:

1) evaluates the feasibility of allocating computing capacity for the Company's IT infrastructure and allocates that capacity;

2) deploys and hosts the Company's IT infrastructure in the Bank's data centers, helps the responsible employee of the Information Technology Department develop and update the Company's information infrastructure diagram, provides up-to-date data, and endorses the diagrams developed;

3) ensures that Company users are granted access to the Company's information systems, except for specialized information systems to which access is granted by the information systems' IT managers;

4) ensures the configuration of the Company's system and application software;

5) ensures compliance with the established requirements for the continuity of information infrastructure operations and the confidentiality, integrity, and availability of information system data, including redundancy and/or archiving and information backups, in accordance with internal service level agreements (SLAs);

6) installs security updates and remediates vulnerabilities on servers.

43. The ISC performs the following information security coordination functions to oversee cooperation between the ISC and the Company and ensure the required and sufficient level of information security:

1) defines information security requirements;

2) endorses internal regulatory documents with respect to information security;

3) endorses proposals to implement organizational measures and information security hardware and software tools;

4) ensures the proper operation of hardware and software tools that automate information security processes and grants access to them;

5) endorses the action plan to implement the Company's strategy with respect to information security;

6) determines resource requirements, including the budget to implement measures to manage information security risks;

7) endorses the required information security activities, specifying implementation deadlines and the persons responsible.

44. Employees who fail to comply with the procedures and rules governing the use of information resources and the Company's information security measures in the performance of their assigned duties are held liable in accordance with the applicable laws of the Republic of Kazakhstan and the Company's internal regulatory documents.

9. Final Provisions

45. The Company's Managing Director/Responsible Person agrees with the Management Board on the introduction of additional controls to suspend some or all of the Company's business processes when the responsible employee of the Information Security Department or the ISC reports that a critical information security incident has been detected and that the Company cannot continue normal operations while guaranteeing the confidentiality, availability, and integrity of information.

46. All matters not addressed in this Policy are resolved in accordance with the laws of the Republic of Kazakhstan, the Company's internal regulatory documents and decisions of its authorized governing bodies, and the Company's established business practices.

47. The Policy takes effect on the date the Board of Directors approves it and ceases to have effect when the Board of Directors repeals it.

48. The applicable laws of the Republic of Kazakhstan take precedence if legislative changes cause any provisions of this Policy to conflict with them. The Policy's nonconflicting provisions continue to apply until the Policy is amended.

49. An employee of the Information Security Department reviews and/or develops this Policy and the Company's regulatory documents on information security matters at least once a year.

Information Security Department