УТВЕРЖДЕНО
Решением Правления
АО «Транстелеком»
от 22 июня 2023 года
№ 15/2023

Политика информационной безопасности АО «Транстелеком»

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее - Политика) является основополагающим документом в области информационной безопасности и служит руководством при разработке соответствующих внутренних нормативных документов в АО «Транстелеком» (далее - Общество).

1.2. Политика разрабатывается в целях реализация бизнес стратегии и бизнес целей Общества.

1.3. Под информационной безопасностью Общество понимает состояние защищенности своих интересов (целей) от угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационных активов Общества: конфиденциальность, целостность и доступность.

1.4. В целях обеспечения безопасности информационно-коммуникационной инфраструктуры в Общество при оказании услуг и решений в области связи, автоматики, энергетики, информационных технологий и информационной безопасности применяется Система менеджмента информационной безопасности (далее - СМИБ). СМИБ распространяется на все структурные подразделения Общества, включая филиалы Общества.

1.5. Общество стремится соответствовать международным требованиям обеспечения информационной безопасности за счет поддержания в рабочем состоянии и развития СМИБ согласно стандарту менеджмента информационной безопасности СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования», а также требованиям законов, стандартов и нормативных требований Республики Казахстан, связанных с информационной безопасностью.

1.6. Обеспечение СМИБ Общества осуществляется в рамках циклической модели (*цикл Деминга «PDCA – Plan-Do-Check-Act»*) менеджмента информационной безопасности: «планирование — реализация — проверка — совершенствование», отвечающей принципам и модели корпоративного менеджмента в Общества.

1.7. Положения Политики распространяются на всех работников Общества, имеющих доступ к информационно-коммуникационной инфраструктуры Общества, а также учитываются в отношениях с контрагентами (потребителями продукции, поставщиками, партнерами, консультантами, стажерами, практикантами и т.д.).

1.8. Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

2. Сфера действии

2.1 Цели Общества в области информационной безопасности

2.1.1 Основной целью СМИБ Общества является обеспечение устойчивого функционирования Общества и надежности используемых информационно-коммуникационной инфраструктуры посредством предотвращения угроз и минимизации уровня рисков в сфере информационной безопасности.

2.1.2 Достижение поставленной цели обеспечивается выполнением Обществом следующих задач:

– обеспечение целостности, непрерывности и доступности информационно-коммуникационной инфраструктуры Общества в целях поддержки высокого качества бизнес-процессов;

– реализация нормативно-правовых, организационно-административных и материально-технических мер по обеспечению информационной безопасности;

– повышение профессиональной квалификации работников в области информационной безопасности;

– эффективное реагирование Общества на современные угрозы и риски в области информационной безопасности;

– соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;

– вовлечение всего персонала в реализацию процесса соблюдения информационной безопасности.

2.2 Принципы реализации Политики

2.2.1 При достижении поставленных целей Общество намерено руководствоваться следующими принципами:

1) **Вовлеченность руководства Общества в процесс обеспечения информационной безопасности** – деятельность по обеспечению информационной безопасности инициирована и контролируется руководством Общества (Председатель Правления, заместители Председателя Правления). Руководство Общества выполняет те же правила по обеспечению информационной безопасности, что и все работники Общества;

2) **Законность обеспечения информационной безопасности** – действия, направленные на обеспечение информационной безопасности в строгом соответствии с действующим законодательством и договорным обязательствами;

3) **Экономическая целесообразность** – Общество стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации;

4) **Знание своих работников** – Общество стремится тщательно подбирать персонал (работников), вырабатывать и поддерживать корпоративную этику, что создает благоприятную среду для деятельности Общества и снижает риски информационной безопасности;

5) **Документированность требований информационной безопасности** – Общества стремится, чтобы все требования в области информационной безопасности были зафиксированы во внутренних нормативных документах, утвержденных руководством Общества;

6) **Осведомленность в вопросах обеспечения информационной безопасности** – документированные требования в области информационной безопасности доводятся до сведения работников Общества и контрагентов в части их касающейся. Общество на периодической основе осуществляет информирование, обучение работников по вопросам обеспечения информационной безопасности;

7) **Реагирование на инциденты информационной безопасности** – Общество стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности;

8) **Персональная ответственность** – работники Общества (всех уровней) несут персональную ответственность за соблюдение требований информационной безопасности. Обязанности по обеспечению информационной безопасности включаются в трудовые договоры и должностные инструкции работников, а также в договоры (соглашения) с контрагентами;

9) **Учет действий с информационными активами** – Общество стремится вести учет всех действий работников Общества и контрагентов в своих информационных активах;

10) **Предоставление минимально необходимых прав доступа** – работникам Общества и контрагентам предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств;

11) **Учет требований информационной безопасности в проектной деятельности** – помимо операционной деятельности, Общество стремится учитывать требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации;

12) **Непрерывность** – мероприятий по обеспечению информационной защиты Общества осуществляется без прерывания текущих бизнес-процессов Общества;

13) **Комплектность** – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла на всех технологических этапах их использования и во всех режимах

функционирования;

14) **Взаимодействие и координация** – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Общества, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями.

15) **Оценка влияния неблагоприятных факторов на цели** – любые возникающие или прогнозируемые угрозы в информационных технологиях должны оцениваться в части их влияния на цели и успешность выполнения бизнес-процессов Общества и должны находить отражение в оценке рисков Общества.

2.3 Документационное обеспечение

2.3.1 Общество разрабатывает и внедряет внутренние нормативные документы по обеспечению информационной безопасности на основе законодательных требований, а также положений международных и национальных стандартов в области информационной безопасности:

– долгосрочную программу мероприятий по обеспечению информационной безопасности;

– планы обеспечения непрерывности бизнеса и действий в случаях чрезвычайных ситуаций.

2.3.2 Кроме того, Общество на периодической основе проводит анализ внутренних нормативных документов на предмет их эффективности и непротиворечивости, а также поддерживает данные документы в актуальном состоянии.

2.3.3 Положения настоящей Политики подлежат пересмотру по результатам проведения внешнего аудита, внутреннего анализа и оценки рисков информационной безопасности для информационно-коммуникационной инфраструктуры Общества, а также в связи с изменением законодательства в области информатизации и кретических инцидентов ИБ, которые затрагивают требования положений Политики информационной безопасности. Политика пересматривается с целью анализа и актуализации изложенной информации (на предмет выявления необходимости в его корректировке) не реже 1 (одного) раза в 2 (два) года.

3. Область действия системы менеджмента информационной безопасностью

Документы, детализирующие требования политики информационной безопасности принятые в Обществе:

1) методика оценки рисков информационной безопасности;

2) правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;

3) правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;

4) правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;

5) правила проведения внутреннего аудита ИБ;

6) правила использования средств криптографической защиты информации;

7) правила разграничения прав доступа к электронным информационным ресурсам;

8) правила использования Интернет и электронной почты;

9) правила организации процедуры аутентификации;

10) правила организации антивирусного контроля;

11) правила использования мобильных устройств и носителей информации;

12) правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов;

13) регламент резервного копирования и восстановления информации;

14) правила организации удаленного доступа к информационным ресурсам;

15) правила обеспечения информационной безопасности при работе с поставщиками;

16) инструкцию о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях;

17) правила работ по инструментальному обследованию;
18) управление информационной безопасностью;
19) руководства администратора по сопровождению объекта информатизации.

4. Ответственность и обязательства

4.1. Руководство Общества:

– принимает участие в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности Общества (бизнеса), законами, нормативными актами, Уставом и внутренними нормативными документами Общества;

– осознает, что информационная безопасность является одним из важнейших факторов успешной и стабильной работы Общества и намерено оказывать необходимое содействие и демонстрировать приверженность целям и принципам обеспечения информационной безопасности. Руководство Общества также оставляет за собой общий надзор за процессом управления информационной безопасностью;

– стремится обеспечить эффективную и стабильную работу Общества, а также поддержать уверенность всех заинтересованных сторон в надежности и стабильности работы Общества, в защищенности их интересов от рисков информационной безопасности;

– стремится к достижению поставленной цели путем создания, поддержки, контроля и постоянному улучшению системы управления информационной безопасностью, основывающейся на сбалансированном комплексе организационных и технических мер по обеспечению информационной безопасности.

4.2. За несоблюдение законов, стандартов и нормативных требований Республики Казахстан, связанных с информационной безопасностью к работникам Общества могут быть применены меры, предусмотренные соответствующими внутренними нормативными документами Общества, трудовыми договорами и действующим законодательством Республики Казахстан, к третьим лицам применяется мера, предусмотренная договором и законодательством Республики Казахстан.

4.3. Все работники Общества несут ответственность за разглашение информации о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, утрату документов, носителей информации содержащих такие сведения, в соответствии с законодательством Республики Казахстан.

4.4. Исполнительный директор, курирующий вопросы информационной безопасности и рисков Общества, отвечает за все аспекты управления безопасностью, в том числе разработку, пересмотр, оценку настоящей Политики, включая принятие решения по управлению рисками.

4.5. Владельцы процессов, отвечают за разработку, пересмотр, оценку документации по ИБ.

4.6. Работники Общества обязаны:

1) знать и соблюдать внутренние требования, обеспечивающие безопасность информационных систем;

2) использовать доступные зарегистрированные защитные механизмы для обеспечения и целостности своей информации;

3) информировать непосредственного руководителя Центрального аппарата/филиала, работников направления внутреннего контроля о нарушениях информационной безопасности и иных подозрительных ситуациях, и инцидентах;

4) в случае обнаружения слабых мест в защите ресурсов информационных систем, незамедлительно сообщать об этом работникам направления внутреннего контроля;

5) выполнять процедуры, необходимые для предупреждения проникновения, обнаружения и уничтожения компьютерного вируса;

6) соблюдать принцип «чистого стола» в отношении бумажных документов, сменных информационных носителей и электронных средств обработки информации.