УТВЕРЖДЕНА
решением Правления
АО «Транстелеком»
2 октября 2019 года
№23/2019____

Политика информационной безопасности АО «Транстелеком»

1. Общие положения

Настоящая Политика является основополагающим документом в области информационной безопасности и служит руководством при разработке соответствующих Положений, Правил и Инструкций.

Для обеспечения безопасности информационно-коммуникационной инфраструктуры в АО «Транстелеком» (далее – 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 АО «Транстелеком».

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».

2. Цели и принципы

Целью информационной безопасности Общества является:

1) обеспечение информационной безопасности при осуществлении деятельности Общества;

2) защита конфиденциальной информации Общества;

3) обеспечение соблюдения законов, стандартов и нормативных требований Республики Казахстан, связанных с информационной безопасностью.

Построение системы обеспечения информационной безопасности Общества и ее функционирование должны осуществляться в соответствии со следующими принципами:

1) законность – действия, направленные на обеспечение информационной безопасности, осуществляются на основе действующего законодательства;

2) ориентированность на бизнес – информационная безопасность рассматривается как процесс основной деятельности Общества;

3) непрерывность – мероприятия по обеспечению информационной защиты Общества должны осуществляться без прерывания текущих бизнес-процессов Общества;

4) комплектность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

5) 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;

6) приоритетность – категорирование всех информационных ресурсов Общества по степени важности при оценке реальных и потенциальных угроз информационной безопасности;

7) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8) специализация – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными работниками;

9) принцип «чистого стола» в отношении бумажных документов и сменных информационных носителей и принцип «чистого экрана» в отношении электронных средств обработки информации;

10) 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;

11) 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;

12) управление доступом – доступ к активам Общества должен быть ограничен в соответствии с должностными обязанностями и актуализироваться в соответствии с результатами анализа рисков информационной безопасности. Предоставление привилегированных прав доступа должно строго ограничиваться и контролироваться;

13) криптографическая защита – криптографические механизмы могут использоваться в Обществе в следующих случаях: использования шифрования для обеспечения конфиденциальности информации при ее хранении или передаче и использование цифровых подписей для защиты аутентичности и целостности хранимой или передаваемой конфиденциальной информации. Криптографические средства должны использоваться в соответствии с релевантными требованиями соглашений, законодательства и нормативных документов;

14) мобильные устройства и носители информации – мобильные устройства и носители информации должны использоваться только для выполнения должностных задач, за внесение несанкционированных изменений в настройки корпоративного мобильного устройства и в носители информации пользователь несет ответственность.

3. Ответственность и обязательства

Эффективная безопасность требует подотчетности, исчерпывающего определения и признания обязанностей в сфере безопасности.

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.

Заместитель Председателя Правления, курирующий вопросы информационной безопасности и рисков Общества, отвечает за все аспекты управления безопасностью, включая принятие решений по управлению рисками.

За несоблюдение законов, стандартов и нормативных требований Республики Казахстан, связанных с информационной безопасностью, к работникам Общества могут быть применены меры, предусмотренные соответствующими внутренними документами Общества, трудовыми договорами и действующим законодательством Республики

Казахстан, к третьим лицам применяется мера, предусмотренная договором и законодательством Республики Казахстан.

Руководство Общества содействует постоянному улучшению системы менеджмента информационной безопасности.

4. Пересмотр Политики информационной безопасности

Положения настоящей Политики подлежат пересмотру по результатам проведения внешнего аудита, внутреннего анализа и оценки рисков информационной безопасности для информационно-коммуникационной инфраструктуры Общества и должны актуализироваться по мере необходимости.

Настоящая Политика информационной безопасности вступает в силу с момента ее утверждения решением Правления Общества и действует до принятия новой Политики информационной безопасности.