REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

1 Введение

Требования настоящей Политики распространяются на всех работников Товарищества при работе в информационных системах.

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

1.1 Политика информационной безопасности ТОО «REGICOM» (далее – Политика) разработана с целью определения стратегических целей, задач и основных требований к комплексу мер в области информационной безопасности, обеспечению устойчивости функционирования информационных систем и сохранности информации, обеспечению всесторонней защиты интересов ТОО «REGICOM» (далее – Товарищество), его контрагентов, а также работников от угроз в сфере информационных технологий.

1.2. В Политике раскрываются основные виды угроз информационной безопасности Товарищества, объекты корпоративной информационной системы Товарищества, на которые направлены данные угрозы, а также требования к мерам защиты от угроз.

1.3. Основные концептуальные задачи по реализации Политики:

1.3.1. планирование, реализация и контроль за выполнением комплекса организационных и технических мер по обеспечению информационной безопасности на основе оценки рисков Товарищества в сфере информационных технологий, направленных на обеспечение:

а) непрерывной доступности информационных активов Товарищества для поддержки его бизнес-процессов;

б) целостности информационных активов Товарищества в целях поддержки высокого качества бизнес-процессов;

в) конфиденциальности информации Товарищества и иных сторон;

г) соответствия предпринимаемых мер по информационной безопасности, применяемых в Товариществе, требованиям законодательства, а также требованиям регулирующих и надзорных органов;

1.3.2. совершенствование системы управления информационной безопасностью, как неотъемлемой части общей системы управления Товарищества, включая:

а) совершенствование организационной структуры, охватывающей все уровни управления в Обществе, начиная с его руководства, и всех процессов системы управления информационной безопасностью;

б) совершенствование процессов системы управления информационной безопасностью, обеспечивающих реализацию выбранного комплекса мер по обеспечению информационной безопасности;

в) обеспечение со стороны руководства Товарищества контроля, оценки результатов и эффективности процессов системы управления информационной безопасностью и предпринимаемых в рамках этих процессов мер по обеспечению информационной безопасности,

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

а также их соответствия установленным требованиям;

1.3.4. документирование требований по информационной безопасности с учетом выбранного комплекса организационных и технических мер;

1.3.5. обеспечение осведомленности работников о политике Товарищества в области информационной безопасности, предпринимаемых мерах, требованиях по обеспечению информационной безопасности, обязанностях и правилах поведения, возлагаемых на работников, а также обеспечение контроля за их надлежащим выполнением;

1.3.6. обеспечение соблюдения требований законодательства Республики Казахстан в ходе деятельности по обеспечению информационной безопасности Товарищества.

1.4. В основу Политики заложены следующие базовые принципы:

1.4.1. своевременность обнаружения неблагоприятных факторов, влияющих на цели Товарищества – система управления информационной безопасностью направлена на быстрое выявление, анализ и прогноз развития угроз в информационных технологиях, способных негативно повлиять на стабильность и надежность работы Товарищества;

1.4.2. 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 Товарищества и должны находить отражение в оценке рисков Товарищества;

1.4.3. приоритетность – требования по информационной безопасности имеют приоритет перед любыми иными требованиями, предъявляемыми к информационным системам и активам Общества;

1.4.4. адекватность – меры организационного и технического характера должны соответствовать рискам – затраты на реализацию этих мер должны быть адекватны прогнозируемому ущербу от реализации угроз в информационных технологиях;

1.4.5. определенность целей – при планировании мер должны устанавливаться четкие и достижимые цели. При документировании требований также должны указываться четкие и ясные цели, которые Общество стремится достичь при выполнении этих требований;

1.4.6. результативность – любые меры по информационной безопасности должны планироваться с учетом результата, которого Общество стремится достичь при реализации соответствующих мер;

1.4.7. использование опыта и лучших практик – деятельность по обеспечению информационной безопасности должна выполняться с учетом накапливаемого и анализируемого опыта, как Общества, так и других организаций, а также с учетом рекомендаций международных стандартов и лучших мировых практик;

1.4.8. непрерывность – деятельность по обеспечению информационной безопасности Общества должна строиться на непрерывной основе как постоянно совершенствующийся процесс, в основе которого лежит система управления информационной безопасностью, охватывающая все бизнес-процессы, все уровни управления и всех работников Общества;

1.4.9. контролируемость и эффективность мер – любые меры должны контролироваться руководством на предмет их соответствия оцениваемым рискам, полноты и качества реализации. Обществом должна оцениваться эффективность мер исходя из степени достижения поставленных целей и результатов;

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

1.4.10. законность – предполагает осуществление защитных мероприятий и разработку системы безопасности информации Общества в соответствии с законодательством Республики Казахстан;

1.4.11. системность - системный подход к построению системы защиты информации и учету всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации;

1.4.12. комплексность – комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано.

1.5. Термины и сокращения

В настоящей Политике используются следующие термины и сокращения:

Таблица 1.5.1.

№	Термин/сокращение	Определение термина / расшифровка сокращения
1.	Товарищество	ТОО «REGICOM»
2.	ДИБ	департамент информационной безопасности
3.	ИБ	информационная безопасность;
4.	Инцидент информационной безопасности, включая нарушения, сбои в КИС (далее - инцидент)	отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов Товарищества;
5.	ИТ	информационные технологии;
6.	КИР	ключевой индикатор риска;
7.	ИС	информационные системы;
8.	Пользователь	работник структурного подразделения Товарищества или иное лицо, использующее ресурсы КИС;
9.	СП	структурное подразделение Товарищества;
10.	СУИБ	система управления информационной безопасностью.

1.6. Нормативные ссылки

В настоящей Политике используются ссылки на следующие нормативные документы:

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

Таблица 1.6.1.

№ п.п	Нормативные документы
Внешние	
	Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V
	Закон Республики Казахстан «О связи» от 5 июля 2004 года № 567-II
	Закон Республики Казахстан «О доступе к информации» от 16 ноября 2015 года № 401-V
	Единые требования в области информационнокоммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832
	Международные стандарты в области информационной безопасности ISO/IEC 27001 Information technology – Code of practice for information security management
Внутренние	
	Положение по коммерческой тайне П RC 06-22

2 Политика является методологической основой для:

2.1. формирования и проведения единой политики в области обеспечения информационной безопасности в информационных системах Товарищества, выработки комплекса согласованных мер организационного, физического и программно-аппаратного характера, направленных на выявление, отражение и ликвидацию последствий реализации угроз информационной безопасности в информационных системах Товарищества;

2.2. координации деятельности структурных подразделений Товарищества при проведении работ по созданию, развитию и эксплуатации информационных систем с соблюдением требований обеспечения информационной безопасности.

3 Участниками системы управления информационной безопасностью Общества являются:

1) Директор ТОО «REGICOM»;

2) привлеченный специалист по обеспечению информационной безопасности;

3) подразделение по работе с персоналом;

4) юридическое подразделение;

5) подразделение внутреннего аудита;

6) владельцы бизнес-процессов и информационных систем.

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

4.1. Доступ к ИС осуществляется на основании матрицы доступа, инициатором создания которой является бизнес-владелец ИС.

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

4.2. Предоставление доступа к ИС Товарищества, отнесенным к категории критичных информационных активов (далее – критичные информационные системы), производится путем формирования и внедрения ролей для обеспечения соответствия прав доступа пользователей ИС их функциональным обязанностям. Совокупность таких ролей представляет собой матрицу доступа к ИС, которая формируется Товариществом в электронной форме или на бумажном носителе.

4.3. Процесс создания и использования матриц доступа в ИС Общества определяется Правилами организации работы в информационных системах ТОО «REGICOM».

4.4. Доступ к ИС осуществляется путем идентификации и аутентификации пользователей ИС.

4.5. Идентификация и аутентификация пользователей ИС Товарищества производится посредством ввода пары «учетная запись (идентификатор) – пароль» или с применением способов двухфакторной аутентификации.

4.6. В ИС Товарищества используются только персонализированные пользовательские учетные записи.

4.7. Использование технологических учетных записей допускается в соответствии с перечнем таких учетных записей для каждой ИС с указанием лиц, персонально ответственных за их использование и актуальность, утверждаемым руководителем подразделения по ИТ по согласованию с привлеченным IT-специалистом.

4.8. В ИС Товарищества применяются функции по управлению учетными записями и паролями, а также блокировке учетных записей пользователей.

4.9. Работникам Товарищества предоставляется доступ к защищаемой, конфиденциальной информации в объеме, необходимом для исполнения их функциональных обязанностей.

4.10. Работники получают доступ к ИС после ознакомления с требованиями ИБ.

4.11. Установка и настройка программного обеспечения и оборудования производится работниками, привлекаемыми по договору.

4.12. Запрещается предоставлять пользователям на рабочих станциях права локального администратора или аналогичные права за исключением случаев, когда такие права необходимы для функционирования программного обеспечения, автоматизирующего функции, исполняемые пользователем.

4.13. При изменении функциональных обязанностей работника отключаются все имеющиеся права доступа и присваиваются новые права доступа, соответствующие его новым функциональным обязанностям.

4.14. При прекращении трудовых отношений с работником отключаются все его права доступа в ИС.

4.15. При длительном отсутствии работника на рабочем месте его доступ в ИС блокируется в порядке, установленным внутренним нормативным документом Общества.

4.16. Привлеченный IT-специалист производит проверку соответствия прав доступа к ИС матрице доступа, а также контроль отключения прав доступа работникам, с которым прекращены трудовые отношения, и блокирования доступа длительно отсутствующим работникам.

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

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

5.1. Товариществом проводится мониторинг деятельности по обеспечению ИБ и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов ИБ.

5.2. Товариществом проводится мониторинг событий ИБ и управление инцидентами ИБ.

5.3. Товарищество определяет перечень событий ИБ, подлежащих мониторингу, источники событий, периодичность их появления, правила мониторинга и методы мониторинга.

5.4. Привлеченный IT-специалист при необходимости вводит дополнительный контроль, частично или полностью останавливает бизнес-процесс, в случае возникновения инцидента ИБ.

5.5. В случае если имеется необходимость мониторинга отдельных источников событий ИБ во внерабочее время, создается круглосуточная служба мониторинга.

5.6. Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные программные средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

5.7. Товарищество пересматривает всю информацию по событию ИБ (источник события, периодичность, правила и методы мониторинга), подлежащих к мониторингу, не реже одного раза в год с учетом имеющейся статистики и эффективности мониторинга.

5.8. Товариществом определяется порядок отнесения события ИБ к инцидентам ИБ.

5.9. Порядок управления инцидентами ИБ определяется Правилами реагирования на инциденты информационной безопасности в ТОО «REGICOM»

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

6.1. Товарищество определяет основные критерии классификации события ИБ как инцидента ИБ.

6.2. Товарищество определяет порядок принятия неотложных мер к устранению инцидента ИБ, его причин и последствий.

6.3. Товарищество определяет порядок информирования о произошедшем инциденте ИБ руководящих работников, привлеченного IT-специалист и Директора.

6.4. Товарищество проводит всесторонний анализ причин возникновения инцидента, его механизма и последствий.

6.5. Для инцидентов ИБ, вероятность возникновения которых высока и отсутствует возможность ее снизить в ближайшем будущем, создаются отдельные документы, описывающие алгоритм обработки инцидента такого рода, типовых неотложных мер по локализации инцидента и его последствий, методов обработки инцидента.

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

6.6. На основании анализа инцидента подготавливается заключение, в котором отражается вся информация об инциденте, а также предложения по проведению корректирующих мер, в целях снижения вероятности и возможного ущерба от повторного инцидента.

6.7. Товарищество ведет журнал учета инцидентов ИБ с отражением всей информации об инциденте, принятых мерах и предлагаемых корректирующих мерах. Допускается ведение журнала, как на бумажном носителе, так и в электронном виде.

6.8. Информация об инцидентах ИБ, полученная в ходе мониторинга деятельности по обеспечению ИБ, подлежит консолидации, систематизации и хранению.

6.9. Срок хранения информации об инцидентах ИБ составляет не менее 5 (пяти) лет.

7 Требования к проведению анализа информации об инцидентах информационной безопасности

7.1. По результатам обработки инцидента ИБ привлеченный IT-специалист проводит всесторонний анализ причин возникновения инцидента ИБ, его механизма и последствий. При сборе данных с программно-технических средств, вовлеченных в инцидент ИБ, обеспечивается сохранность и неизменность собранных данных.

7.2. По результатам анализа готовится заключение в произвольной форме, в котором отражается вся информация об инциденте ИБ, а также предложения по принятию корректирующих мер, в целях снижения вероятности и возможного ущерба от повторного инцидента ИБ.

7.3. Для инцидентов ИБ, вероятность возникновения которых высока и не может быть снижена в короткие сроки, разрабатываются документы, описывающие алгоритм обработки таких инцидентов ИБ, типовых неотложных мер по локализации инцидента ИБ и его последствий, методов обработки инцидента ИБ.

7.4. Результаты анализа инцидентов ИБ, а также рекомендации по минимизации вероятности возникновения инцидентов ИБ и их возможного ущерба ежегодно выносятся на рассмотрение Директора и в дальнейшем используются для оценки рисков ИБ, корректировки методов и средств обеспечения ИБ, изменения бизнес-процессов.

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

8.1. Несоблюдение требований настоящей Политики влечет ответственность в соответствии с законодательством Республики Казахстан и внутренними документами Товарищества.

8.2. Привлеченный IT-специалист несет ответственность за реализацию положений Политики, координацию и взаимодействие СП, мониторинг эффективности СУИБ.

8.3. Привлеченный IT-специалист несет ответственность за поддержание работоспособности ИС и систем их защиты, используемых в Товарищества.

8.4. Все работники Товарищества несут ответственность за неразглашение информации о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и утрату документов, изделий и магнитных носителей, содержащих такие сведения, в соответствии с законодательством Республики Казахстан.

8.5. Работники Товарищества обязаны:

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

1) знать и соблюдать внутренние требования, обеспечивающие безопасность ИС;

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

3) информировать непосредственного руководителя отдела, Директора о нарушениях ИБ и иных подозрительных ситуациях и инцидентах;

4) в случае обнаружения слабых мест в защите ресурсов ИС, незамедлительно сообщать об этом привлеченному IT-специалисту;

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

9 Намерения Руководства

9.1. Руководство Товарищества стремится обеспечить эффективную и стабильную работу Товарищества, а также поддержать уверенность всех заинтересованных сторон в надежности и стабильности работы Товарищества, в защищенности их интересов от воздействия различных неблагоприятных факторов.

9.2. К руководству Товарищества относятся:

1) Директор ТОО «REGICOM»

9.3. Эффективная деятельность руководства является одним из критичных факторов успешной и стабильной работы Товарищества и намерено оказывать необходимое содействие и демонстрировать приверженность целям и принципам обеспечения ИБ. Руководство Товарищества также оставляет за собой общий надзор за процессом управления ИБ.

9.4. Руководство Товарищества стремится к достижению поставленной цели путем создания, поддержки, контроля и развития эффективной СУИБ, основывающейся на сбалансированном комплексе организационных и технических мер по обеспечению ИБ.

9.5. Обеспечение ИБ Товарищества достигается реализацией комплекса необходимых процессов и мер, поддерживаемых каждым работником Товарищества в необходимой и определенной для него мере в соответствии с положениями внутренних документов по обеспечению ИБ Товарищества.

9.6. Руководство стремится организовать деятельность по обеспечению ИБ в соответствии со стандартами, такими как СТ РК ISO 9001:2015 и лучшими практиками.

10 Меры защиты обеспечения информационной безопасности

10.1. Обеспечение ИБ предусматривает реализацию комплекса организационных, правовых, физических и аппаратно-программных мер защиты.

10.2. Организационные (административные) меры обеспечения ИБ - это меры организационного характера в Товариществе (издание соответствующих внутренних документов Товарищества), обеспечивающие регламентацию процессов функционирования ИС, использование ресурсов ИС, деятельность технического персонала, а также порядок взаимодействия пользователей с ИС таким образом, чтобы затруднить или исключить возможность реализации угроз ИБ или снизить размер потерь в случае их реализации.

10.3. Правовые меры обеспечения ИБ заключаются в применении норм законодательства Республики Казахстан.

REGICOM в Казахстане
Адрес: Республика Казахстан, г. Алматы, 050046,
проспект Абылай хана, д.122/64, оф.12
БИН 200840024949
Контакты: +7 (701) 786 82 79 , +7 (727) 267-31-20
E-mail: regicom@mail.ru
Сайт: www.regicompany.com

10.4. Физические меры обеспечения ИБ предполагают использование специализированных механических, электро- и электронно-механических устройств и сооружений для создания физических препятствий на возможных путях доступа нарушителей к компонентам ИС, а также для предотвращения физических повреждений аппаратных средств ИС вследствие воздействия техногенных факторов (пожаров, затоплений и пр.).

10.5. Аппаратно-программные меры обеспечения ИБ заключаются в применении различных электронных устройств и специальных программ, входящих в состав ИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическую защиту информации и т. д.).

10.6. Соблюдение правил обеспечения ИБ, включающих процедуры по обеспечению сохранности информации о сведениях, составляющих коммерческую тайну, и недопущению их использования в собственных интересах брокером и (или) дилером, их работниками или третьими лицами. Правилами обеспечения ИБ в рамках регуляторной деятельности определяются:

1) порядок составления, оформления, регистрации, учета и хранения документов, содержащих информацию, относящуюся к коммерческой тайне;

2) порядок допуска к перечню информации, относящейся к коммерческой тайне, с указанием работников Товарищества, которые допускаются к данной информации;

3) механизмы предотвращения утечки информации, составляющих коммерческую тайну, и искажения информационных данных, предусматривающих: - перечень информационных данных, имеющий ограниченный доступ; - порядок получения доступа; - порядок контроля доступа к информационным данным, установление перечня должностей, имеющих доступ к информационным данным;

4) мероприятия по предотвращению несанкционированного использования CRM-системой Товарищества, управления автоматизированной базой данных и обеспечения системой, позволяющей идентифицировать личность пользователя.

11 Внесение изменений и дополнений в Политику

11.1. Внесение изменений и дополнений в Политику осуществляется в соответствии с требованиями Правил по управлению внутренними нормативными документами Товарищества.

11.2. Ответственность за внесение изменений в Политику несет Директор.

11.3. Если в результате изменения законодательства Республики Казахстан нормы настоящей Политики вступают в противоречие с действующим законодательством, эти нормы Политики утрачивают силу и до момента внесения изменений, дополнений в настоящую Политику необходимо руководствоваться действующим законодательством Республики Казахстан.

11.4. Содержание настоящей Политики должно быть доведено до сведения работников Товарищества в порядке, определенном нормативными документами и процедурами Товарищества.

11.5. Контроль за ознакомлением с настоящей Политикой возлагается на Ответственного за подготовку и разработку документов по поддержанию СМК.