NATD	**Акционерное общество «Национальное агентство по технологическому развитию»**		
Вид документа: **Политика**	Код документа:	Ред.	Кол-во страниц:
Разработал: Иманбаева Б.	Одобрено: решением Правления АО «НАТР» от «___»_____2014г. №__	Утверждено: Решением Совета директоров АО «НАТР» от _____ 201_ г. Протокол №____	

ПОЛИТИКА О КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ АО «НАЦИОНАЛЬННОЕ АГЕНТСТВО ПО ТЕХНОЛОГИЧЕСКОМУ РАЗВИТИЮ»

Астана 2014

Информация о документе	
Название документа	Политика о конфиденциальной информации АО «НАТР»
Название файла	
Тип документа	Microsoft Word

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика о конфиденциальной информации (далее – Политика) в акционерном обществе «Национальное агентство по технологическому развитию» (далее – Агентство) разработана в соответствии с действующим законодательством Республики Казахстан, Уставом, Кодексом корпоративного управления и внутренними документами Агентства.

2. Определения и сокращения, используемые в Политике:

1) безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования;

3) доступность – возможность для авторизованного пользователя информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью;

4) информационная безопасность (ИБ) – комплекс административно-правовых, организационно-распорядительных и технических мер, направленных на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи и хранения;

5)информационная система (ИС) обработки информации – организационно-техническая структура, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных;
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;
- баз данных на различных носителях;
- персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных;

6) коммерческая тайна – не являющаяся государственным секретом информация, имеющая ценность в силу ее неизвестности третьим лицам, в отношении которой Агентством введен режим коммерческой тайны (способы управления Агентством, сведения о финансах, сведения, изложенные в бухгалтерской и налоговой отчетности, научно-техническая,

технологическая, производственная, финансово-экономическая или иная информация, переговоры с партнерами, заявителями, грантополучателями, проектными компаниями, заседания Бюджетной комиссии, Правления, Совета Директоров, переговоры по проектам между подразделениями, работниками Агентства в том, числе в устной форме и т.д.);

7)конфиденциальная информация – служебная и коммерческая тайны, свободный доступ к которой имеют лица в силу служебной необходимости;

8)конфиденциальность – защита от несанкционированного ознакомления;

9)несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации;

10)общедоступной информацией - признается информация, не относящаяся к сведениям, составляющим конфиденциальную или иную охраняемую законом тайну, а также информация, подлежащая обязательному публичному раскрытию.

11) пользователь – субъект, пользующийся информацией, полученной от её собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

12) работник – лица, работающие по трудовым, гражданско-правовым договорам, заключенным с Агентством;

13) разглашение конфиденциальной информации – передача в устной, письменной, электронной или иной форме, раскрытие и подобные действия, совершенные работником умышленно или по неосторожности, включая халатное отношение к своим должностным обязанностям, повлекшие ознакомление со сведениями, составляющими коммерческую тайну, любых лиц, не имеющих права доступа к указанным сведениям без согласия Агентства;

14) сеть (локальная сеть, ЛВС, LAN) – группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающее соединение станций и передачу между ними информации;

15) служебная тайна – несекретные сведения, касающиеся внутренней организации деятельности Агентства, доступ к которым ограничен в силу служебной необходимости, в том числе содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных, электронных и иных сообщениях, передаваемых по сетям Интернет, электронной и почтовой связи, которые стали известны работнику Агентства в связи с исполнением трудовых обязанностей и ограничение на распространение которой диктуется служебной необходимостью;

16)угроза – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта;

17) уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

3. Политика предусматривает защиту конфиденциальной информации, предупреждения причинения Агентству ущерба, вызванного неправомерными действиями физических и юридических лиц по незаконному получению, распространению и использованию конфиденциальной информации Агентства, подходы к раскрытию информации; перечень общедоступных документов, информации (материалов), подлежащих раскрытию всем заинтересованным лицам вне зависимости от цели их получения, а также вопросы, связанные с информационной безопасностью.

4. Действие настоящей Политики распространяется на работников Агентства, взявших на себя обязательство о неразглашении коммерческой и служебной тайны, в порядке и на условиях, предусмотренной настоящей Политикой.

5. Действие Политики не распространяется на отношения, связанные с обращением со сведениями, составляющими государственные секреты в соответствии с законодательством Республики Казахстан.

6. Ответственность за соблюдение требований Политики в структурных подразделениях несут руководители структурных подразделений Агентства и курирующие члены Правления.

7. Текущий контроль за соблюдением работниками, (за исключением Председателя Правления и его заместителей) требований Политики при работе с конфиденциальной информацией осуществляют руководители структурных подразделений.

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

8. Сведения, составляющие конфиденциальную информацию Агентства, определены перечнями согласно Приложениям № 1 и № 2 соответственно к настоящей Политике.

9. При внесении изменений и дополнений в указанные перечни сведений, составляющие конфиденциальную информацию влечет обязательное ознакомление работников с внесенными изменениями и дополнениями под роспись. В противном случае обязательства работника по сохранению конфиденциальной информации остаются в прежнем виде.

10. Не составляют коммерческой тайны сведения, относящиеся к государственной статистической отчетности, а также касающиеся тех сторон

деятельности Агентства, которые выступают объектом государственного контроля и надзора.

2.1. ЗАЩИТА КОНФИДЕНЦАЛЬНОЙ ИНФОРМАЦИИ

11. Отнесение сведений к конфиденциальной информации осуществляется путем введения в предусмотренном настоящей Политике порядке ограничений на разглашение и доступ к ее носителям.

12. Отнесение сведений к коммерческой тайне осуществляется в соответствии с принципами обоснованности и своевременности. Обоснованность заключается в установлении целесообразности отнесения конкретных сведений к коммерческой тайне. Своевременность заключается в установлении ограничений на разглашение этих сведений с момента их получения (разработки) или заблаговременно до указанного момента.

13. В исключительных случаях, не терпящих отлагательства, отнесение сведений к коммерческой тайне осуществляется путем проставления первым руководителем Агентства, либо лицом, осуществляющим его обязанности грифа «Конфиденциально», с последующим оформлением этих сведений в порядке, предусмотренном настоящей Политикой. В данном случае указанные сведения приобретают статус коммерческой тайны с момента проставления указанного грифа.

14. В целях защиты конфиденциальной информации в течение 5 (пяти) календарных дней с даты назначения (избрания) работника Агентства (члена Совета директоров):

1) ответственное лицо Агентства по кадровой работе обеспечивает подписание с работником Обязательства о неразглашении конфиденциальной информации (далее – Обязательство) по форме согласно Приложению №3 к настоящей Политике;

2) корпоративный секретарь обеспечивает подписание независимыми директорами и иными членами Совета директоров Обязательства о неразглашении по форме согласно приложению к положению о Совете директоров Агентства.

15. Работник обязан неукоснительно соблюдать требования указанные в Приложение № 3 к настоящей Политике.

16. В работе с контрагентами (юридическими и физическими лицами) Агентством при необходимости защиты конфиденциальной информации заключаются соглашения или договоры о конфиденциальности либо в условиях договора предусматриваются положения о неразглашении конфиденциальной информации.

2.3. ДОПУСК К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

17. К сведениям, составляющим конфиденциальную информацию, имеют допуск следующие лица:

1) единственный акционер – неограниченный допуск на основании письменных запросов и в рамках материалов по вопросам, вынесенным на его рассмотрение;

2) члены Совета директоров и Председатель Правления – неограниченный допуск на основании их письменных запросов и в рамках материалов по вопросам, вынесенным на заседания Совета директоров Агентства;

3) члены Правления, работники Агентства и физические лица, оказывающие услуги Агентству – в рамках выполнения возложенных на них функций;

4) государственные органы Республики Казахстан – в порядке и на условиях, установленных законодательством Республики Казахстан.

18. Все работники Агентства при приеме на работу в обязательном порядке подписывают Обязательства о неразглашении конфиденциальной информации и ознакамливаются со сведениями составляющих служебную и коммерческую тайну.

19.Работники других юридических лиц и физические лица, не являющиеся работниками Агентства, могут быть допущены к ознакомлению и работе с конфиденциальными документами по решению Председателя Правления при наличии:

1) соглашения или договора о конфиденциальности между этими организациями и Агентством либо если в заключенном между организациями и Агентством договоре содержатся условия о неразглашении конфиденциальной информации;

2) мотивированного письменного запроса тех организаций, в которых они работают, с указанием темы выполняемого задания, фамилии, имени и отчества работника.

2.4. ПОРЯДОК ПРЕКРАЩЕНИЯ ДОПУСКА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

20. Допуск работника к конфиденциальной информации может быть прекращен в следующих случаях:

1) расторжения трудового договора (независимо от причин расторжения);

2) однократного нарушения им взятых на себя обязательств, связанных с неразглашением и защитой коммерческой и служебной тайны;

21. Прекращение допуска осуществляется по решению Председателя Правления Агентства, которое оформляется в виде приказа в письменной форме и доводится до сведения работника под роспись.

3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3.1. ЦЕЛИ, ЗАДАЧИ И ОСНОВОПОЛАГАЮЩИЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

22. Основной целью информационной безопасности является защита корпоративной ИС Агентства от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, минимизация уровня рисков, порядок раскрытия информации, а также защиты конфиденциальной информации, предупреждения причинения Агентству ущерба, вызванного неправомерными действиями физических и юридических лиц по незаконному получению, распространению и использованию конфиденциальной информации Агентства.

23. Основными задачами системы информационной безопасности являются:

1) ограниченное распространение банковской, конфиденциальной информации, подлежащей защите от неправомерного использования;

2) прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Агентства, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

3) создание условий функционирования Агентства с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;

4) создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Агентства, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;

5) создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц.

24. Построение системы обеспечения безопасности информации Агентства и её функционирование должны осуществляться в соответствии со следующими основными принципами:

1) законности – соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;

2) системности – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Агентства;

3) эффективности – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению ИБ должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;

4) целесообразности – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;

5) непрерывности – принцип функционирования системы информационной безопасности, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;

6) взаимодействии и координации – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами ответственных подразделений Агентства;

7) совершенствовании – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

8) приоритетности – категорирование (*ранжирование*) всех информационных ресурсов Агентства по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;

9) информированности и персональной ответственности – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационные сервисы индивидуально идентифицирует пользователей и инициируемые ими процессы;

10) соответствие стандартам – система информационной безопасности соответствует международным стандартам в данной области;

11) обязательность контроля – контроль за деятельностью пользователей, а также мониторинг работы ИС должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия;

12) регулярности и своевременности раскрытия информации обязательность контроля – раскрытия информации означает ответственность Агентства в отношении соблюдения сроков и системности предоставления информации, предусмотренной действующим законодательством и внутренними документами;

13) открытости и доступности информации - выбор таких каналов распространения информации, доступ к которым является для заинтересованных сторон свободным, необременительным и малозатратным, а также намерение Агентства обеспечить максимальную прозрачность информации о своей деятельности с учетом соблюдения режима конфиденциальности по отношению к информации, составляющей служебную, коммерческую и иную охраняемую законом тайну. Выбор Агентством таких каналов распространения информации, доступ к которым является для заинтересованных сторон свободным, необременительным и малозатратным, а также намерение Агентства обеспечить максимальную прозрачность информации о своей деятельности с учетом соблюдения режима конфиденциальности по отношению к информации, составляющей служебную, коммерческую и иную охраняемую законом тайну;

14) достоверности и полноты – предоставление Единственному Акционеру и другим заинтересованным сторонам информации, соответствующей действительности и достаточной для понимания в полном объеме раскрываемого факта или события;

15) оперативности – предоставление наиболее существенной информации, касающейся особо значимых фактов и событий, затрагивающих интересы Единственного акционера и других сторон, в том числе при необходимости принятия ими соответствующих решений, в максимально сжатые сроки.

3.2. ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

25. Объектами обеспечения информационной безопасности является конфиденциальная информация, а также следующие элементы автоматизированной системы обработки информации Агентства:

1) информация, необходимая для обеспечения нормального функционирования Агентства (*далее – защищаемая информация*);

2) средства и системы информатизации (*средства вычислительной техники, информационно-вычислительные комплексы, сети, системы*), на

которых производится обработка, передача и хранение защищаемой информации;

3) программные средства (*операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение*) автоматизированной системы Агентства, с помощью которых производится обработка защищаемой информации;

4) помещения, предназначенные для ведения закрытых переговоров и совещаний;

5) помещения, в которых расположены средства обработки защищаемой информации;

6) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

26. Подлежащая защите информация может находиться:

1) на бумажных носителях;

2) в электронном виде (*обрабатываться, передаваться и храниться средствами вычислительной техники*);

3) передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

4) в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;

5) записываться и воспроизводиться с помощью технических средств (*диктофоны, видеомагнитофоны и др.*).

3.3. РИСКИ (УГРОЗЫ) ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

27. Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

1) утрата сведений, составляющих конфиденциальную информацию Агентства и иную защищаемую информацию, а также искажение (*несанкционированная модификация, подделка*) такой информации;

2) утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (*несанкционированный доступ, копирование, хищение и т.д.*), а также утечка информации по каналам связи и за счёт побочных электромагнитных излучений;

3) недоступность информации в результате её блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

4) отсутствие планирования и контроля;

5) низкая степень надёжности программного обеспечения;

6) недостаточная осведомлённость персонала, низкая квалификация персонала и пользователей в области информационных технологий.

28. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Агентства и его нормальное функционирование:

1) финансовые потери, связанные с утечкой или разглашением защищаемой информации;

2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

3) ущерб от дезорганизации деятельности Агентства и потери, связанные с невозможностью выполнения им своих обязательств;

4) моральные потери (*ущерб репутации Агентства*).

29. В случае реализации рискового события (*угрозы реализации*), Агентство обязано немедленно уведомить Единственного акционера о выявленных инцидентах, касающихся информационной безопасности Агентства.

3.4. ПРОГРАММА СОЗДАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ

30. Политика служит методологической основой для формирования и реализации программы создания системы информационной безопасности Агентства. В целом для функционирования системы информационной безопасности с учётом положений Политики должны быть разработаны и утверждены Правлением Агентства (с учётом необходимого обновления) документы организационно-распорядительного характера, регламентирующие порядок обеспечения сохранности конфиденциальной информации в рамках каждой функциональной задачи и соответствующей ей автоматизированной системы.

31. В процессе создания системы безопасности необходимо предусмотреть приоритеты реализации наиболее важных и актуальных направлений обеспечения безопасности, с учетом выделяемых финансовых ресурсов.

32. В целях достижения оптимального уровня информационной безопасности следует:

1) иметь в наличие внутренний документ, определяющий требования к защите конфиденциальной информации, включающий описание процедур отнесения сведений к категории конфиденциальных и, в случае необходимости, в установленном порядке вносить в него изменения и дополнения;

2) регулярно проводить анализ принятой технологии обработки конфиденциальной информации, включая категорирование ресурсов по степени критичности обрабатываемых с их помощью данных;

3) определять полный перечень и возможные угрозы нарушения конфиденциальности информации и классифицировать их по вероятности возникновения исходя из принятой типовой модели нарушителя;

4) с учётом действующих мер и средств защиты проводить оценку риска утечки конфиденциальной информации;

5) разработать и внедрить систему обеспечения безопасности информации в Агентстве (*систему защиты информации*), направленную на снижение уровня риска, включающую комплекс организационных мер и технических средств;

6) на постоянной основе проводить обучение и повышение квалификации персонала Агентства в области информационной безопасности;

7) проводить периодический контроль эффективности и адекватности принимаемых мер защиты информации.

4. ПОРЯДОК РАЗМЕЩЕНИЯ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ

33. Политика Агентства по раскрытию информации направлена на достижение наиболее полной реализации прав Единственного акционера на получение информации, существенной для принятия им инвестиционных и управленческих решений, а также на защиту информации об Агентстве, разглашение которой способно нанести ущерб Агентству и его Единственному акционеру.

34. Общедоступная информация, должна быть размещена Агентством на корпоративном веб-сайте не позднее 1 (одного) месяца со дня наступления соответствующего события либо же в течение 1 (одного) месяца со дня обновления/поступления информации либо же должна раскрываться в сроки и в порядке, установленные действующим законодательством Республики Казахстан.

35. В случае обращения представителей средств массовой информации, Агентство обязано представить запрашиваемую информацию в порядке и сроки, предусмотренные законодательством Республики Казахстан о средствах массовой информации.

36. Председатель Правления Агентства вправе уполномочивать работников для выступления от имени Агентства или подготовки и направления ответов на конкретные запросы. Работники, не являющиеся уполномоченными представителями, не должны отвечать на запросы по предоставлению информации об Агентстве, если им это не было непосредственно поручено Председателем Правления.

37. Агентство вправе организовывать не реже 1 (одного) раза в год или по мере необходимости брифинги (пресс-конференции) в связи с опубликованием очередной финансовой отчетности, решениями Единственного акционера и другими значимыми корпоративными событиями.

4.1. РАЗМЕЩЕНИЕ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ НА КОРПОРАТИВНОМ ВЕБ-САЙТЕ АГЕНСТВА

38. Агентство раскрывает на корпоративном веб-сайте следующую общедоступную информацию:

1) устав Агентства, изменения и дополнения в него;
2) кодекс корпоративного управления;
3) положение о Совете директоров;
4) положение о дивидендной политике;
5) список аффилированных лиц;
6) годовой отчёт Агентства;
7) финансовая отчетность, в том числе консолидированная, составленные в соответствии с законодательством Республики Казахстан о бухгалтерском учете и финансовой отчетности, и заключение аудиторов по данной отчетности;
8) кредитная история и кредитные рейтинги, присвоенные Агентству;
9) презентации (текст, слайды) по видам деятельности Агентства;
10) тексты, а при наличии видео- и аудиозаписи публичных выступлений должностных лиц Агентства;
11) проспект выпуска ценных бумаг, изменения и дополнения в него в случаях, предусмотренных нормативными правовыми актами Республики Казахстан;
12) информация о дочерних организациях;
13) иные сведения, определяемые государственным органом, осуществляющим регулирование и надзор финансового рынка и финансовых организаций, а также органами Агентства.

39. Агентство по решению Председателя Правления может разместить на корпоративном веб-сайте следующую дополнительную информацию:

показатели деятельности Агентства;
структуру органов Агентства;
новости;
пресс-релизы;
контактную информацию;
иную информацию в соответствии с положениями внутренних документов Агентства.

4.2. ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ ЕДИНСТВЕННОМУ АКЦИОНЕРУ

40. Агентство обязано доводить до сведения Единственного акционера информацию о следующих корпоративных событиях общества:

Информацией, затрагивающей интересы Единственного акционера Агентства, признаются:

1) решения, принятые Единственным акционером и советом директоров по перечню вопросов, информация о которых в соответствии с внутренними документами Агентства должна быть доведена до сведения акционеров и инвесторов;

2) выпуск обществом акций и других ценных бумаг и утверждение уполномоченным органом отчетов об итогах размещения ценных бумаг общества, отчетов об итогах погашения ценных бумаг Агентства, аннулирование уполномоченным органом ценных бумаг Агентства;

3) совершение обществом крупных сделок и сделок, в совершении которых у Агентства имеется заинтересованность;

3-1) передача в залог (перезалог) имущества Агентства на сумму, составляющую пять и более процентов от активов Агентства;

4) получение обществом займа в размере, составляющем двадцать пять и более процентов от размера собственного капитала Агентства;

5) получение обществом лицензий на осуществление каких-либо видов деятельности, приостановление или прекращение действия ранее полученных обществом лицензий на осуществление каких-либо видов деятельности;

6) участие Агентства в учреждении юридического лица;

7) арест имущества общества;

8) наступление обстоятельств, носящих чрезвычайный характер, в результате которых было уничтожено имущество общества, балансовая стоимость которого составляла десять и более процентов от общего размера активов Агентства;

9) привлечение Агентства а и его должностных лиц к административной ответственности;

9-1) возбуждение в суде дела по корпоративному спору;

10) решения о принудительной реорганизации Агентства;

11) иные события, затрагивающие интересы Единственного акционера и инвесторов, в соответствии с уставом общества, а также проспектом выпуска ценных бумаг Агентства.

41. Агентство обязано предоставить в адрес Единственного акционера информацию о корпоративных событиях в течении 5 рабочих дней с даты ее возникновения, информация о возбуждении в суде дела по корпоративному спору должна быть предоставлена в течение 7 рабочих дней с даты получения Агентством судебного извещения.

42. По итогам работы за год Агентство разрабатывает и направляет на утверждение Единственному акционеру годовой отчет Агентства.

43. Годовой отчет Единственному акционеру Агентства должен содержать необходимую информацию, позволяющую Единственному акционеру оценить итоги деятельности Агентства за год:

1) приоритетные направления деятельности Агентства и результаты развития Агентства по приоритетным направлениям его деятельности;

2) раздел о корпоративном управлении;

3) оценка позиции Агентства и перспектив его развития;

4) существенные риски, связанные с деятельностью Агентства;

5) перечень совершенных Агентством в отчетном году сделок, признаваемых крупными в соответствии с законодательством Республики Казахстан и Уставом Агентства;

6) краткие сведения о членах Совета директоров и Правления Агентства (*когда впервые был назначен, его возраст, профессия, основное место работы, гражданство, а также иные должности, которые он занимает*), включая их квалификацию, процесс отбора, в том числе о независимых директорах с указанием критериев определения их независимости, а также об изменении состава Совета директоров и Правления Агентства, сведения о размере вознаграждений членов Совета директоров;

7) количество заседаний Совета директоров и его Комитетов, а также посещение каждым из членов Совета директоров заседаний Совета директоров и Комитета, в состав которого он входит;

8) отчет Совета директоров Агентства о результатах развития Агентства по приоритетным направлениям его деятельности;

9) отчет о работе Комитетов по выполнению ими функций, в том числе, с указанием причин отклонения Советом директоров отдельных предложений и/или рекомендаций Комитетов;

10) отчет о работе Совета директоров и Правления, включая полную информацию по вопросам, по которым решения принимаются Советом директоров или Правлением, а также вопросам, решения по которым делегированы Председателю Правления;

11) процесс проведения оценки деятельности Совета директоров, Комитетов, отдельных членов Совета директоров, Правления, Службы внутреннего аудита;

12) принятые меры по учету Советом директоров мнения Единственного акционера в отношении Агентства (*с помощью непосредственного общения, брифингов*);

13) сведения о соблюдении Кодекса корпоративного управления и Кодекса корпоративной этики;

14) существенные вопросы, связанные с заинтересованными лицами;

15) любая финансовая поддержка, включая гарантии, принятые на себя Агентством;

16) информация об акциях Агентства, в том числе о выпусках акций;

17) информация о выплате объявленных (*начисленных*) дивидендов по акциям Агентства, а если дивиденды не были выплачены - о причинах их невыплаты;

18) иную информацию.

44. Годовой отчет должен быть подписан Председателем Правления Агентства, руководителями структурных подразделений по корпоративному и экономическому развитию и главным бухгалтером, и предварительно утвержден Советом директоров Агентства.

45. Агентство представляет годовой отчет на рассмотрение Единственному акционеру вместе с материалами по утверждению Единственным акционером годовой финансовой отчетности.

46. Агентство после утверждения Единственным акционером годового отчета, в течение 20 (*двадцати*) календарных дней публикует его на корпоративном веб-сайте.

4.3. РАСКРЫТИЕ ИНФОРМАЦИИ ЗАИНТЕРЕСОВАННЫМ ЛИЦАМ

47. Агентство предоставляет заинтересованным лицам информацию, не отнесенную Политикой к конфиденциальной и иной охраняемой законом тайне, согласно порядку и срокам, предусмотренным Законом Республики Казахстан «О порядке рассмотрения обращений физических и юридических лиц».

48. Информация, в том числе конфиенциальная, по запросам государственных, правоохранительных органов предоставляется на основании действующего законодательства Республики Казахстан

5. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

49. За нарушение обязательств о неразглашении коммерческой тайны работник несет ответственность, предусмотренную ст.200 Уголовного кодекса РК, ст. 158 Кодекса об административных правонарушениях РК, а так же трудовым договором, заключенным с Агентством.

50.За нарушение обязательств о неразглашении служебной тайны работник несет ответственность, предусмотренную трудовым законодательством Республики Казахстан.

51. В случае разглашения конфиденциальной информации работник обязан возместить Агентству причиненные этим убытки. Размер нанесенного

ущерба определяет специальная комиссия, с участием всех заинтересованных структурных подразделений Агентства.

52. При обнаружении в действиях работника признаков состава преступления Агентство по инициативе направляет соответствующее сообщение в правоохранительные органы.

Приложение № 1
к Политике о конфиденциальной информации АО «НАТР»

ПЕРЕЧЕНЬ
сведений, составляющих коммерческую тайну
АО «Национальное агентство по технологическому развитию»

1) сведения о состоянии банковских счетов и проводимых по ним операциях;

2) сведения о результатах переговоров с партнерами;

3) сведения переговоров между сотрудниками Агентства по проектам;

4) сведения, составляющие коммерческую тайну других юридических и физических лиц, полученных на основании договоров (*соглашений*);

5) содержание сделок с другими юридическими и физическими лицами, банками второго уровня, если иное прямо не предусмотрено в договорах (*соглашениях*), заключаемых по указанным сделкам;

6) сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры;

7) технические сведения об инновационных разработках дочерних и зависимых организаций, клиентов и их дочерних и зависимых организаций;

8) содержание первичных документов и регистров бухгалтерского учета;

9) сведения, касающиеся рассмотрения, реализации инвестиционных проектов, а также участия в венчурных фондах, включающие в себя: заявки, бизнес-планы, технико-экономические обоснования, проектно-сметная документация, отчеты по оценке активов и др.

10) договора и информация по условиям заключения договоров по поставкам оборудования, осуществления строительно-монтажных работ и других товаров, работ и услуг.

11) соглашения и информация по условиям заключения соглашений по совместной реализации инвестиционных проектов с инициаторами (заявителями) проектов.

12) информация о принимаемых решениях органами АО "НАТР", касающиеся деятельности проектных компаний и венчурных фондов.

13) аудиозапись заседаний органов АО "НАТР" и прочих заседаний, а также рабочих встреч, проводимых для решения текущих задач в рамках реализации инвестиционных проектов, а также участия в венчурных фондах.

14) переписка, в том числе через интернет ресурсы, осуществляемая в рамках реализации инвестиционных проектов, а также участия в венчурных фондах.

15) информация о мнениях, высказанных работниками Агентства, в ходе обсуждения вопросов, связанных с реализацией инвестиционных проектов и участия в венчурных фондах.

16) архивная информация об инвестиционных проектах, в которых приостановлена деятельность либо осуществлен выход Агентства.

17) отчеты по этапам работ по инновационным проектам (ТБИ, гранты).

18) сведения, изложенные в бухгалтерской и налоговой отчетности.

19) заседания Бюджетной комиссии, Правления, Совета Директоров переговоры по проектам между подразделениями, работниками Агентства в том, числе в устной форме и т.д.

Приложение № 2
к Политике о конфиденциальной информации АО «НАТР»

ПЕРЕЧЕНЬ
сведений, составляющих служебную тайну
АО «Национальное агентство по технологическому развитию»

1) сведения о заработной плате работников, штатное расписание, используемая система мотивации;
2) информация о работниках, персональные данные работников, их домашние адреса, телефоны, состав семьи;
3) сведения о порядке защиты конфиденциальной информации;
4) сведения о способах защиты электронных данных;
5) сведения об организации охранной деятельности;
6) материалы служебных расследований;
7) сведения по хранению и использованию печатей и штампов;
8) информация о внутренних процедурах финансовых подразделений Агентства;
9) сведения содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных, электронных и иных сообщениях, передаваемых по сетям Интернет, электронной и почтовой связи, которые стали известны работнику Агентства в связи с исполнением трудовых обязанностей и ограничение на распространение которой диктуется служебной необходимостью.

Приложение № 3
к Политике о конфиденциальной информации АО «НАТР»

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации акционерного общества «Национальное агентство по технологическому развитию»

Я, _____

Ф.И.О., должность работника

обязуюсь:

1) строго хранить ставшую мне известной в связи с моей работой в АО «Национальное агентство по технологическому развитию» (далее – Агентство) конфиденциальную информацию Агентства в соответствии с перечнем конфиденциальной информации согласно приложению к Инструкции по защите конфиденциальной информации (далее – Инструкция);

1) не разглашать конфиденциальную информацию Агентства, которая мне доверена или станет известна по работе, в том числе не передавать третьим лицам и не раскрывать публично конфиденциальную информацию без согласия председателя правления Агентства;

2) сохранять информацию, составляющую коммерческую тайну тех организаций, с которыми у Агентства имеются деловые отношения;

3) выполнять требования Политики о конфиденциальной информации и иных внутренних документов Агентства, приказов, распоряжений руководства Агентства по обеспечению сохранности конфиденциальной информации Агентства;

4) не использовать конфиденциальную информацию в личных целях, не связанных с выполнением моих трудовых (служебных) обязанностей, в том числе другой деятельностью, которая в качестве конкурентного действия может нанести ущерб Агентству;

5) в случае попытки третьих лиц (в том числе иных работников Агентства) получить от меня конфиденциальную информацию агентства незамедлительно известить об этом соответствующее должностное лицо;

6) немедленно сообщать непосредственному руководителю (руководителю структурного подразделения, Заместителю Председателя Правления, Председателю Правления) и лицу, ответственному за учет и хранение документов, содержащих конфиденциальную информацию, об утрате или недостаче носителей конфиденциальной информации,

удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации;

7) при увольнении передать непосредственному руководителю все носители конфиденциальной информации (документы, чертежи, рукописи, магнитные ленты, распечатки, диски и т.д.), которые находились в моем распоряжении в связи с выполнением служебных обязанностей во время работы;

8) в случае увольнения в течение 5 (пяти) лет не разглашать и не использовать для себя или других лиц конфиденциальную информацию Агентства;

9) не предпринимать никаких действий по получению сведений, указанных в перечне конфиденциальной информации согласно приложению 1 и 2 к Политике не связанных с моими трудовыми (служебными) обязанностями.

10) представлять непосредственному руководителю информацию (документы), подготовленную при выполнении мной трудовых (служебных) обязанностей и предназначенную для передачи третьим лицам, для ее оценки на предмет отнесения к конфиденциальной информации.

11) Я уведомлен (-а) о том, что в случае нарушения мной данного обязательства:

- буду привлечен (-а) к дисциплинарной ответственности, вплоть до увольнения с работы;

- буду обязан (-а) возместить убытки, понесенные Агентством в связи с разглашением или использованием мной в личных целях сведений, составляющих конфиденциальную информацию Общества, как в период работы в Обществе, так и в течение 5 (*пяти*) лет после увольнения.

Подпись _____

«____»_____ 201_ г.

ПРИЛОЖЕНИЕ 1

ЛИСТ ОЗНАКОМЛЕНИЯ

Должность	Фамилия, инициалы	Дата	Роспись

ПРИЛОЖЕНИЕ 2

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№№ п\п	№№ раздела, пункта стандарта	Дата введения изменения	Основание (№,дата приказа)	Дата внесения изменения	Подпись лица, внесшего изменение

Контроль изменений документа			
версия	Описание изменения	Автор	Дата утверждения

6. ПРИЛОЖЕНИЯ

№	Название	Кол-во страниц
1	Лист ознакомления	
2	Лист регистрации изменений	
3	Приложение №1	
4	Приложение №2	
5	Приложение №3	

Разработано:

Заместитель директора Центра правового и административного обеспечения — Б.Иманбаева

СОГЛАСОВАНО:

Заместитель Председателя Правления — Р.Касымбеков

Управляющий директор – Директор Центра экономического развития — Е. Тапишев

Управляющий директор – Директор Центра корпоративного развития и стимулирования инновационной активности — Б.Айтілеу