

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила охраны конфиденциальности инсайдерской информации и контроля за соблюдением требований Федерального закона от 27.07.2010 года № 224-ФЗ "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" (далее - Закон об инсайте) Открытого акционерного общества «GTL» (далее - Правила) разработаны в соответствии с указанным Законом, нормативными правовыми актами Федерального органа исполнительной власти по рынку ценных бумаг, иным законодательством Российской Федерации, в целях обеспечения соблюдения порядка использования инсайдерской информации, повышения уровня доверия к Открытому акционерному обществу «GTL» (далее - Общество) со стороны инвесторов и контрагентов Общества, а также в целях охраны инсайдерской информации Общества от неправомерного использования.

1.2. Настоящие Правила определяют систему охраны и контроля за соблюдением мер, направленных на:

- ✓ предотвращение неправомерного использования сведений, составляющих инсайдерскую информацию,
- ✓ ограничение круга лиц, имеющих доступ к инсайдерской информации,
- ✓ определение сравнительного анализа конъюнктуры по направлениям возможного использования инсайдерской информации,
- ✓ выявление фактов использования такой информации, наказание виновных.

1.3. Доступ к инсайдерской информации осуществляется только в соответствии с установленным в Обществе порядком.

1.4. Ответственным за обеспечение охраны конфиденциальности инсайдерской информации и контроля за соблюдением требований Закона об инсайте является Президент Общества.

2. СИСТЕМА ОХРАНЫ И КОНТРОЛЯ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

3.1. Система охраны и контроля инсайдерской информации, режима сохранения конфиденциальности инсайдерской информации включает следующие направления:

- ✓ идентификация и учет лиц, владеющих инсайдерской информацией,
- ✓ установление пропускного режима в отдельные помещения, занимаемые Обществом, в том числе в нерабочие дни,
- ✓ нанесение на материальные носители (документы), содержащие инсайдерскую информацию, соответствующих грифов, ограничивающих доступ к ним,
- ✓ своевременное уничтожение всех не подлежащих хранению документов, которые содержат инсайдерскую информацию,
- ✓ разрешение доступа к инсайдерской информации только в определенных Обществом местах,
- ✓ обеспечение защиты рабочих мест и мест хранения документов от беспрепятственного доступа и наблюдения,
- ✓ обеспечение защиты информационно-технических систем от потери информации и несанкционированного доступа к информации, в том числе по каналам связи,
- ✓ контроль за функционированием системы управления рисками и оценка рисков:
 - выявление и анализ внутренних (сложность организационной структуры, уровень квалификации сотрудников, организационные изменения, текучесть кадров и т.д.) и внешних (изменение экономических условий деятельности Общества, применяемые технологии и т.д.) факторов, оказывающих воздействие на деятельность Организации,
 - оценка рисков в Организации на предмет несанкционированного использования инсайдерской информации,
 - ✓ контроль за управлением информационными потоками (получением и передачей информации) и обеспечением информационной безопасности:
 - общий контроль компьютерных систем (контроль за главным компьютером, системой сервера и рабочими местами конечных пользователей и т.д.), проводимый с целью обеспечения бесперебойной и непрерывной работы,
 - программный контроль встроенными в прикладные программы автоматизированными процедурами, а также выполняемыми вручную процедурами, контролирующими обработку финансово-

хозяйственных операций и других сделок (контрольное редактирование, контроль логического доступа, внутренние процедуры резервирования и восстановления данных и т.п.),

- организационный контроль в соответствии с установленным в Обществе режимом охраны коммерческой тайны, порядком защиты от несанкционированного доступа и распространения конфиденциальной информации, а также от использования конфиденциальной информации в личных целях,

✓ наблюдение за функционированием системы контроля инсайдерской информации в целях оценки степени ее соответствия задачам деятельности Общества, выявления недостатков, разработки предложений и осуществления контроля за реализацией решений по совершенствованию системы контроля инсайдерской информации Общества.

3. ПРАВИЛА ПРОВЕДЕНИЯ ПРОВЕРОК СОБЛЮДЕНИЯ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

3.1. Контроль за соблюдением требований настоящих Правил, Закона об инсайте, нормативных правовых актов Федерального органа исполнительной власти по рынку ценных бумаг и иного законодательства РФ осуществляет лицо, состоящее в штате Общества на должности Специалиста по контролю инсайдерской информации (далее - Специалист), который назначается Президентом Общества.

Специалист по контролю инсайдерской информации подотчетен Совету директоров Общества.

3.2. Общество обязано обеспечить условия для беспрепятственного и эффективного осуществления Специалистом по контролю инсайдерской информации своих функций.

3.3. Специалист по контролю инсайдерской информации осуществляет следующие функции:

✓ составляет и ведет список инсайдеров Общества в соответствии с Законом об инсайте,
✓ уведомляет в порядке, установленном нормативными правовыми актами Федерального органа исполнительной власти в области финансовых рынков, лиц, включенных в список инсайдеров, об их включении в такой список и исключении из него, информирует лиц о требованиях Закона об инсайте,

✓ передает в порядке, установленном нормативными правовыми актами Федерального органа исполнительной власти в области финансовых рынков, список инсайдеров Общества организаторам торговли, через которые совершаются операции с финансовыми инструментами, иностранной валютой и (или) товаром,

✓ передает список инсайдеров Общества в уполномоченный Федеральный орган исполнительной власти в области финансовых рынков (далее - ФСФР) по его требованию, рассматривает письменные запросы ФСФР и предоставляет требуемые документы, объяснения, информацию в срок, указанный в запросах,

✓ разрабатывает меры по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и/или манипулированию ценами на ценные бумаги Общества,

✓ осуществляет проверки соблюдения настоящих Правил, Закона об инсайте, нормативных правовых актов Федерального органа исполнительной власти по рынку ценных бумаг и иного законодательства РФ,

✓ представляет Совету директоров Общества отчеты о своей деятельности в порядке и сроки, устанавливаемые Советом директоров Общества,

✓ представляет Совету директоров и Президенту Общества информацию о выявленных нарушениях Закона об инсайте и рекомендации по их устранению,

✓ осуществляет консультации и методологическую помощь сотрудникам Общества по вопросам своей компетенции,

✓ осуществляет иные функции, необходимые для обеспечения контроля за соблюдением требований настоящих Правил, Закона об инсайте, нормативных правовых актов Федерального органа исполнительной власти по рынку ценных бумаг и иного законодательства РФ.

3.4. Для контроля соблюдения режима конфиденциальности инсайдерской информации Специалист по контролю инсайдерской информации имеет право осуществлять соответствующие проверки.

3.5. Основными методами осуществления проверок соблюдения режима

конфиденциальности инсайдерской информации являются:

- ✓ мониторинг информационной безопасности;
- ✓ оценка надежности учета и отчетности;
- ✓ проверка соблюдения Обществом законодательства Российской Федерации (о конкуренции, о рынке ценных бумаг и др.), внутренних документов Общества и установленных ими методик, программ, правил, порядков и процедур, целью которой является оценка качества и соответствия созданных в Обществе систем обеспечения соблюдения требований законодательства Российской Федерации и иных актов;

операционная проверка, цель которой заключается в оценке качества и соответствия систем, процессов и процедур, анализе организационных структур и их достаточности для выполнения возложенных функций;

проверка качества управления, цель которой состоит в оценке качества подходов органов управления, подразделений и сотрудников общества к рискам и методам контроля за ними в рамках поставленных целей Организации.

3.6. Специалист при проведении проверок имеет право:

- ✓ входить в помещения проверяемого подразделения, а также в помещения, используемые для хранения документов (архивы), ценных бумаг, товаров, валюты, наличных денег и ценностей, обработки данных (компьютерные залы) и хранения данных на машинных носителях, с соблюдением процедур доступа, определенных внутренними документами Общества;
- ✓ получать документы и копии с документов и иной информации, а также любых сведений, имеющихся в информационных системах Общества, необходимых для осуществления контроля, с соблюдением требований законодательства Российской Федерации и требований Общества по работе со сведениями ограниченного распространения;
- ✓ привлекать при осуществлении проверок сотрудников Общества и требовать от них обеспечения доступа к документам, иной информации, необходимой для проведения проверок,
- ✓ обращаться в органы государственной власти и к организаторам торговли по вопросам своей компетенции.

3.7. План проведения проверок, осуществляемых Специалистом, должен включать график осуществления проверок и составляться исходя из принятой органами управления Общества методологии оценки управления рисками, учитывающей изменения в системе контроля инсайдерской информации. При составлении графика осуществления проверок должна учитываться установленная в Обществе периодичность проведения проверок по направлениям деятельности структурных подразделений и Общества в целом.

3.8. План проведения проверок, осуществляемых Специалистом, предусматривает разработку отдельной программы проверки каждого направления (вопроса) деятельности Общества.

3.9. Отчеты и предложения по результатам проверок представляются Специалистом Совету директоров Общества и Президенту Общества.

Отчеты должны содержать описание целей проверки, выполненных работ, выявленных нарушений, ошибок и недостатков в деятельности Общества, которые могут создать угрозу интересам акционеров Общества или оказать влияние на финансовую устойчивость Общества, и рекомендации Специалиста по улучшению работы и устранению нарушений, ошибок и недостатков.

4. ХРАНЕНИЕ ДОКУМЕНТОВ И ИНЫХ НОСИТЕЛЕЙ, СОДЕРЖАЩИХ ИНСАЙДЕРСКУЮ ИНФОРМАЦИЮ И КОНТРОЛЬ ЗА ПОРЯДКОМ ДОПУСКА И РАБОТЫ С НИМИ

4.1. Хранение документов и иных носителей инсайдерской информации осуществляется в помещении места нахождения единоличного исполнительного органа Общества - Президента.

4.2. Хранение и выдачу носителей инсайдерской информации, а также контроль за порядком допуска и работы с инсайдерской информацией, осуществляет Специалист по контролю инсайдерской информации, который назначается приказом Президента Общества и руководствуется положениями заключенного с ним трудового договора и настоящих Правил

4.3. Документы со сведениями, относящимися к инсайдерской информации Общества, оформляются и учитываются в соответствии с принятым порядком документооборота в Обществе.

4.4. Обработка, хранение и защита персональных данных, доступ к которым получен в результате работы с документами и иными носителями, содержащими инсайдерскую информацию, осуществляется в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», иными правовыми актами Российской Федерации, внутренними документами Общества.

5. ВЗАИМОДЕЙСТВИЕ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

5.1. Сотрудники подразделений Общества должны оказывать Специалисту по контролю инсайдерской информации содействие в осуществлении им своих функций.

5.2. Сотрудники Общества, которым стали известны факты нарушения режима конфиденциальности инсайдерской информации, законности и правил совершения операций (сделок), а также факты нанесения ущерба Обществу, контрагентам, обязаны довести эти факты до сведения своего непосредственного руководителя и Специалиста по контролю инсайдерской информации.

6. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ

6.1. Лица, нарушившие требования настоящих Правил, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.