«УТВЕРЖДЕНО»
Приложение №11
к протоколу заседания
Наблюдательного совета
Акционерное общество
«Компания по развитию
предпринимательства»
от «___» апреля 2024 года
№ 6/24

ИНСТРУКЦИЯ
об информационной безопасности Акционерного общества «Компания по развитию предпринимательства»

“ВНЕСЕНО”
Исполнительным органом
АО «Компания по развитию
предпринимательства»

Ташкент – 2024 год

Неофициальный перевод. *Только для справочных целей.*

СОДЕРЖАНИЕ

Примечание:

Настоящий документ является неофициальным переводом оригинального документа на узбекском языке и предоставляется исключительно для справочных целей. В случае расхождений приоритет имеет оригинальная версия документа на узбекском языке.

I. Общие положения

1. Настоящая Инструкция разработана в соответствии с «Положением об информационной политике» АО «Компания по развитию предпринимательства» (в дальнейшем именуемое – Общество), а также с «Положением об организации защиты конфиденциальной информации эмитентами» (от 24.02.2010 г. №2081) и определяет порядок отнесения информации к перечню конфиденциальной информации, а также организацию её защиты.

2. В настоящей Инструкции используются следующие основные понятия:

Конфиденциальная информация - документированная информация, использование которой ограничивается в соответствии с нормативными правовыми актами;

Коммерческая тайна - информация, обладающая коммерческой ценностью в силу своей неизвестности третьим лицам в научно-технической, технологической, производственной, финансово-экономической и других сферах, которая на законных основаниях не используется в свободном обороте и в отношении которой её владелец принимает меры по сохранению конфиденциальности;

Инсайдерская информация – это конкретная и точная информация, которая не была раскрыта или представлена, и которая может оказать существенное влияние на цену финансовых инструментов или продукции Общества в случае её раскрытия или представления. К такой информации относятся, в том числе, коммерческая, служебная, банковская тайна, тайна связи (в части сведений о переводе денежных средств через почту), а также иные охраняемые законом тайны.

II. Критерии отнесения информации к категории конфиденциальной информации

3. К категории конфиденциальной информации относятся коммерческая тайна, инсайдерская информация, а также иная информация с ограниченным доступом.

4. Коммерческая тайна должна обладать следующими признаками:

обладать реальной или потенциальной коммерческой ценностью для своего владельца вследствие неизвестности третьим лицам;

не содержать признаков государственной тайны и других тайн, охраняемых законом;

не быть общедоступной или общеизвестной в соответствии с

законодательством;

обеспечена меры по защите её конфиденциальности.

5. К другой информации с ограниченным доступом относятся следующие сведения:

1) Информация о производственной деятельности Общества, являющаяся коммерческой тайной Общества:

а) Сведения о производственных мощностях Общества;

б) Сведения о технологических процессах;

в) Сведения о планах по расширению или прекращению производства;

д) Производственная конфиденциальная информация Общества (ноу-хау);

е) Информация о выводе на рынок новых видов продукции, товаров, работ и услуг;

ж) Стратегия тарифной политики.

2) Информация о финансово-хозяйственной деятельности Общества:

а) Сведения о хозяйственных договорах, заключённых между Обществом и поставщиками материальных ресурсов на приобретение продукции, товаров, выполнение работ или оказание услуг;

б) Сведения о хозяйственных договорах, заключённых между Обществом и потребителями на поставку продукции, товаров, выполнение работ или оказание услуг;

в) Сведения о финансовых операциях Общества;

г) Протоколы и отчёты службы внутреннего аудита Общества;

д) Акты проверок финансово-хозяйственной деятельности Общества, проведённых государственными контрольными органами;

е) Информация, относящаяся к Обществу как к участнику рынка ценных бумаг;

ж) Сведения об акционерах Общества (личные данные физических лиц и реквизиты юридических лиц, не предназначенные для общего пользования);

з) Сведения о типе и количестве акций, принадлежащих акционерам Общества, за исключением информации, подлежащей обязательному раскрытию;

и) Сведения о типе и количестве корпоративных облигаций, находящихся в собственности владельцев ценных бумаг Общества;

к) Решения органов управления Общества — до их раскрытия эмитентом в порядке, установленном законодательством;

л) Любая информация о деятельности Общества как акционерного общества, не предназначенная для общего пользования;

м) Любая информация, предоставляемая акционерам Общества и недоступная для общего пользования другими лицами;

н) Реестр акционеров Общества;

о) Реестр владельцев корпоративных облигаций Общества;

п) Зарегистрированный список участников общего собрания акционеров Общества;

р) Приказы Директора Общества;

с) Отчёты аудитора Общества;

т) Акты проверок деятельности Общества на рынке ценных бумаг, проведённые уполномоченным государственным органом, регулирующим рынок ценных бумаг.

III. Порядок включения информации, коммерческой тайны, сведений, влияющих на изменение стоимости акций, а также другой информации с ограниченным доступом Общества в перечень конфиденциальной информации

6. Информация, являющаяся коммерческой тайной, а также сведения, раскрытие или предоставление которых может оказать существенное влияние на цену финансовых инструментов или товаров Общества, включаются в перечень конфиденциальной информации (далее — Перечень) в порядке, установленном настоящей Инструкцией.

7. Ведение Перечня осуществляется главным бухгалтером, юрисконсультом и другими ответственными должностными лицами.

8. Для принятия решения о включении информации в Перечень конфиденциальной информации Директору Общества предоставляются следующие документы:

документ, подтверждающий, что информация имеет фактическую или потенциальную коммерческую ценность для Общества в связи с её неизвестностью третьим лицам;

сведения о том, что информация не является общедоступной или общеизвестной в соответствии с законодательством и что её конфиденциальность обеспечена мерами по защите тайны.

9. Представленная информация рассматривается, и решение о её включении в Перечень или исключении из него принимается директором Общества.

10. Руководитель осуществляет постоянный мониторинг информации, включённой в Перечень.

11. В случае выявления по результатам мониторинга информации, не соответствующей критериям, установленным в пункте 3 настоящей Инструкции, директор Общества принимает решение об исключении такой информации из перечня.

IV. Использование конфиденциальной информации сотрудниками Общества и другими лицами

12. Конфиденциальной информацией Общества могут пользоваться следующие лица:

а) Директор Общества;

б) Члены Наблюдательного совета Общества, имеющие право пользоваться конфиденциальной информацией в целях выполнения возложенных на них обязанностей по управлению Обществом;

в) Лица, владеющие не менее чем 25 процентами голосующих акций Общества;

г) Лица, имеющие право использовать конфиденциальную информацию Общества на основании заключённого с Обществом договора, включая аудиторов (аудиторские организации), оценщиков (на основании трудовых договоров, заключённых оценщиками с юридическими лицами), профессиональных участников рынка ценных бумаг, кредитные организации, страховые компании;

д) Лица, осуществляющие присвоение рейтинга Обществу, а также его ценным бумагам;

е) Сотрудники, имеющие право пользоваться конфиденциальной информацией Общества в соответствии со своими должностными обязанностями, включая сотрудников службы внутреннего аудита Общества;

ж) Иные лица — в случаях и порядке, установленных законодательством.

13. В целях учёта лиц, имеющих право пользоваться конфиденциальной информацией Общества, необходимо организовать ведение Перечня лиц, имеющих доступ к конфиденциальной информации Общества.

14. Отдел делопроизводства является ответственным структурным подразделением, осуществляющим ведение Перечня и контроль за обращениями, связанными с использованием конфиденциальной информации.

15. Выдача архивных документов, содержащих конфиденциальную информацию, осуществляется только на основании списка лиц, имеющих разрешение на использование архивных документов с конфиденциальной информацией, утверждённого приказом Директора Общества.

16. При соблюдении следующих условий Директор Общества

предоставляет соответствующим лицам разрешение на использование конфиденциальной информации Общества:

а) Оформление письменного обязательства сотрудника о сохранении и неразглашении сведений, составляющих конфиденциальную информацию;

б) Ознакомление сотрудника с требованиями законодательства по обеспечению защиты конфиденциальной информации.

17. Сотрудникам разрешается доступ к сведениям, составляющим конфиденциальную информацию, исключительно в рамках их должностных обязанностей и только в том объёме, который необходим для надлежащего выполнения этих обязанностей.

18. Директор Общества несёт ответственность за законность разрешений, выданных сотрудникам на использование сведений, составляющих конфиденциальную информацию.

19. Лица, использующие конфиденциальную информацию, обязаны:

а) строго сохранять в тайне сведения, отнесённые к конфиденциальной информации;

б) соблюдать требования законодательства по обеспечению защиты конфиденциальной информации;

в) работать только с теми сведениями и документами, содержащими конфиденциальную информацию, к которым они имеют право доступа;

г) не использовать конфиденциальную информацию в личных целях;

д) незамедлительно сообщать своему непосредственному руководителю или Директору Общества о попытках посторонних лиц получить доступ к конфиденциальной информации от сотрудников, о фактах утраты или недостачи конфиденциальной информации в бумажном или электронном виде, о пропаже или недостаче ключей от помещений, в которых хранятся документы, содержащие конфиденциальную информацию, от хранилищ и сейфов, а также о других обстоятельствах, которые могут привести к разглашению конфиденциальной информации, включая причины и условия возможной утечки;

е) При прекращении трудовых отношений с лицом, имеющим доступ к конфиденциальной информации (в случае увольнения), он обязан передать своему непосредственному руководителю или Директору Общества всю имеющуюся в его распоряжении конфиденциальную информацию в бумажной и электронной форме, связанную с исполнением служебных обязанностей;

ж) Сотрудник также может нести иные обязанности в соответствии с требованиями законодательства.

20. На следующий день после прекращения трудовых отношений с лицом, имеющим право доступа к конфиденциальной информации, Общество

обязано исключить данного человека из Перечня.

21. Директор Общества должен принять необходимые меры для исключения доступа к конфиденциальной информации тех сотрудников, которым не требуется ознакомление при исполнении их должностных обязанностей.

V. Организация обеспечения защиты конфиденциальной информации

22. Общество обязано принимать необходимые меры по защите конфиденциальной информации в соответствии с требованиями законодательства.

23. Защита конфиденциальной информации, осуществляемая Обществом, направлена на предотвращение её утечки, кражи, потери, повреждения, ограничения доступа, подделки и иного несанкционированного использования, а также на предотвращение несанкционированных действий по уничтожению, ограничению доступа, копированию и повреждению информации, а также иных вмешательств в информационные ресурсы и системы профессионального участника.

24. Организация и осуществление контроля за защитой конфиденциальной информации возлагается на Отдел комплаенс-контроля и безопасности Общества (далее — ответственный отдел Общества).

25. Организация защиты конфиденциальной информации Общества осуществляется с соблюдением следующих требований:

а) Формирование и организация конфиденциальной информации Общества, ознакомление каждого сотрудника Общества с перечнем конфиденциальной информации и оформление подписанного обязательства о неразглашении конфиденциальной информации, установление ответственности за разглашение конфиденциальной информации в внутренних документах Общества, трудовых договорах и должностных инструкциях сотрудников;

б) Ограничение использования конфиденциальной информации;

в) Требования к учёту, хранению и работе с конфиденциальной информацией;

г) Требования по защите конфиденциальной информации в структурных подразделениях Общества;

д) Требования к помещениям, в которых расположены технические

средства обработки конфиденциальной информации;

е) Требования к помещениям для хранения документов, содержащих конфиденциальную информацию, с обеспечением необходимого уровня сохранности;

ж) Требования к техническим средствам, на которых хранится и обрабатывается конфиденциальная информация;

з) Требования к программному обеспечению Общества;

и) Требования к контролю за защитой конфиденциальной информации Общества;

к) Требования к раскрытию конфиденциальной информации Общества.

VI. Учёт, хранение и работа с конфиденциальной информацией

26. Конфиденциальная информация Общества может содержаться в текущих документах и архивных материалах.

Конфиденциальная информация может содержаться на бумажных и электронных носителях (электронные документы, копии баз данных, текстовые, табличные и графические файлы), отражающих конфиденциальные сведения.

27. Учёт, хранение и работа с текущими документами, содержащими конфиденциальную информацию, осуществляется в структурных подразделениях Общества в соответствии с внутренним регламентом.

Учёт документов, содержащих конфиденциальную информацию, ведётся в соответствующих журналах в бумажном и (или) электронном виде.

Архивные бумажные документы хранятся в архиве Общества в течение сроков, установленных законодательством.

28. Документы Общества, содержащие конфиденциальную информацию, подлежат передаче в архив Общества не позднее 3 (трёх) месяцев после окончания соответствующего финансового года.

29. Архивные документы, содержащие конфиденциальную информацию, должны храниться в архивном помещении Общества в металлических шкафах и (или) сейфах с надёжными замками и пломбами (маркировками) на время нерабочих часов.

30. Хранение архивных документов, содержащих конфиденциальную информацию, в местах, не предназначенных для хранения данного вида документов, запрещается.

31. Работа с архивными документами, содержащими конфиденциальную информацию, осуществляется исключительно в служебных помещениях.

32. Отправка документов, содержащих конфиденциальную информацию, по почте осуществляется в порядке, установленном законодательством.

33. Ознакомления с архивными документами, содержащими конфиденциальную информацию, оформляется в карточках учета выдачи архивных документов (дел), а также в журнале учета документов, содержащих конфиденциальную информацию.

34. Документ, содержащий конфиденциальную информацию, может быть размножен, скопирован, тиражирован или его содержание может быть раскрыто только в случаях, предусмотренных законодательными актами, и на основании письменного разрешения Директора Общества.

35. Уничтожаемые документы, содержащие конфиденциальную информацию, до передачи на переработку как бумажные отходы, должны быть измельчены до такой степени, чтобы исключить возможность прочтения текста, либо сожжены в специально отведённом месте.

36. После уничтожения документов, содержащих конфиденциальную информацию, в журнал учёта вносится соответствующая отметка.

37. Эмитент при использовании информационно-коммуникационных технологий (далее – ИКТ) обязан принять необходимые меры для защиты конфиденциальной информации от утечки и несанкционированного использования.

38. Вход в помещения, где размещены ИКТ, обрабатывающие конфиденциальную информацию, и базы данных, разрешается только лицам, имеющим соответствующее разрешение на доступ.

39. Лица, использующие ИКТ и обслуживающие их:

а) обязаны выполнять установленные требования по обеспечению защиты конфиденциальной информации при использовании ИКТ;

б) обязаны соблюдать установленный порядок ограничения доступа к конфиденциальной информации;

в) обязаны незамедлительно сообщать своему непосредственному руководителю или Директору Общества о всех попытках несанкционированного использования конфиденциальной информации, а также о фактах её утечки или искажения.

40. Подключение ИКТ к общедоступным системам допускается только при наличии производственной необходимости и исключительно при использовании средств защиты информации.

41. В случае выхода из строя или списания ИКТ, обрабатывающих

конфиденциальную информацию, необходимо принять меры по полному уничтожению содержащихся в них данных с целью недопущения их восстановления.

VII. Требования по обеспечению защиты конфиденциальной информации в структурных подразделениях Общества

42. Сотрудники структурных подразделений Общества при работе с конфиденциальной информацией на бумажных и электронных носителях обязаны обеспечивать учёт и сохранность.

43. К структурным подразделениям Общества, использующим конфиденциальную информацию в процессе работы, предъявляются следующие требования:

а) хранение документов, содержащих конфиденциальную информацию, в специально предназначенных металлических шкафах и (или) сейфах;

б) соблюдение внутреннего регламента по работе с документами, содержащими конфиденциальную информацию;

в) бумажные документы, находящиеся на рабочем столе сотрудников Общества, не должны быть доступны для ознакомления посторонним лицам;

г) При покидании рабочего места (в обеденный перерыв, в перерывах на работе, при уходе с работы) не допускать оставления без присмотра документов, содержащих конфиденциальную информацию;

д) при выходе из кабинета бумажные документы помещаются в закрывающийся ящик рабочего стола, а по окончании рабочего дня — в закрывающиеся металлические шкафы и (или) сейфы, находящиеся в помещении соответствующего структурного подразделения Общества;

е) копирование и внесение изменений в бумажные документы осуществляется с строгим соблюдением внутреннего регламента Общества, при этом ведётся регистрация и учёт всех операций копирования и изменения;

ж) уничтожение бумажных документов осуществляется с строгим соблюдением внутреннего регламента;

з) осуществление руководителем структурного подразделения контроля за использованием его сотрудниками документов, содержащих конфиденциальную информацию, и соблюдением установленных в Обществе требований.

VIII. Требования к помещениям, в которых размещены технические средства обработки конфиденциальной информации

44. В Обществе должен быть составлен перечень помещений, в которых размещены технические средства обработки конфиденциальной информации (производственные помещения, бухгалтерия, юридическая служба, отдел корпоративных отношений с акционерами и другие помещения структурных подразделений Общества).

45. Помещения Общества, в которых размещены технические средства обработки конфиденциальной информации, должны соответствовать следующим требованиям:

а) установка в данных помещениях металлических дверей, запирающихся на замок;

б) оснащение помещений средствами охранной и пожарной сигнализации;

в) соблюдение в данных помещениях соответствующего режима эксплуатации технических средств обработки конфиденциальной информации (температурный режим, уровень влажности и другие требования, установленные для эксплуатации технических средств);

г) ограничение свободного доступа посетителей и посторонних лиц в данные помещения;

д) наличие мер защиты, предотвращающих несанкционированное подключение к техническим средствам обработки конфиденциальной информации.

IX. Требования к хранилищам, обеспечивающим надлежащее хранение документов, содержащих конфиденциальную информацию

46. Документы Общества, содержащие конфиденциальную информацию, подлежат хранению в специально предназначенном помещении — Архиве Общества, где также хранятся другие архивные документы, относящиеся к деятельности Общества.

47. В Архиве Общества должно быть обеспечено надлежащее хранение документов, содержащих конфиденциальную информацию.

48. К Архиву Общества предъявляются следующие требования:

а) установка в помещении архива Общества металлических дверей,

запирающихся на замок;

б) наличие металлических решёток на окнах;

в) оснащение архивных помещений средствами охранной и пожарной сигнализации;

г) соблюдение в данных помещениях установленного порядка хранения документов (температурный режим, уровень влажности и другие условия, указанные в требованиях надлежащего хранения);

д) оснащение архива Общества металлическими шкафами и/или сейфами;

е) наличие отдельного сейфа для хранения застрахованных копий особо важных документов Общества;

ж) ограничение свободного доступа посетителей и посторонних лиц в архив Общества.

X. Требования к программному обеспечению Общества

49. В целях обеспечения информационной безопасности и защиты конфиденциальной информации необходимо соблюдать следующие требования к программному обеспечению Общества (системному, сетевому и прикладному):

а) соответствующее системное программное обеспечение, поддерживающее функционирование системной среды (операционная система серверов, рабочих станций и др.);

б) соответствующее сетевое программное обеспечение, обеспечивающее функционирование локальной (внутренней) сети Общества;

в) соответствующее прикладное программное обеспечение, обеспечивающее функционирование прикладных программ;

г) наличие соответствующей документации, относящейся к прикладному программному обеспечению;

д) возможность ограничения уровня доступа пользователей к прикладному программному обеспечению;

е) наличие возможности резервного копирования прикладной базы данных;

ж) надлежащее хранение и учёт прикладной базы данных;

з) защита информации от утечки, повреждения и несанкционированного доступа посторонних лиц;

и) наличие порядка восстановления информации.

50. При работе с конфиденциальной информацией на электронных

носителях её защита обеспечивается следующими мерами:

а) запрещение несанкционированного доступа к информации;

б) защита от несанкционированного копирования, изменения и уничтожения;

в) защита информации от утраты и повреждения;

г) специальные и профилактические мероприятия.

Защита электронной информации от несанкционированного доступа:

а) пароль для включения компьютера;

Каждая рабочая станция (компьютер пользователя) должна быть защищена паролем для включения (входа). Сотрудники Общества обязаны не разглашать введённый пароль другим лицам.

б) ограничение доступа к сетевым ресурсам;

Сетевой администратор на основании уведомления руководителя структурного подразделения Общества устанавливает доступ сотрудников к сетевым ресурсам в соответствии с их должностными обязанностями.

в) ограничение доступа к функциям прикладного программного обеспечения и баз данных;

Доступ к функциям прикладного программного обеспечения и баз данных устанавливается администратором прикладных баз в соответствии с должностными обязанностями сотрудников.

г) создание и работа с электронными документами осуществляется только с использованием сертифицированных электронных ключей;

д) шифрование и защита паролями отдельных файлов, содержащих конфиденциальную информацию.

Защита электронной информации от несанкционированного копирования, изменения и удаления:

а) специальная защита возможностей копирования, изменения и удаления файлов;

б) копирование и изменение электронной информации осуществляется только в соответствии с «Порядком копирования конфиденциальной информации»;

в) удаление электронной информации осуществляется только в соответствии с «Порядком уничтожения документов, содержащих конфиденциальную информацию».

Защита электронной информации от потери и повреждения:

а) Использование серверов, рабочих станций, сетевого оборудования и других технических средств осуществляется с строгим соблюдением

«Порядка использования средств вычислительной техники и технического оборудования»;

б) Работы, выполняемые в электронной базе данных, осуществляются с строгим соблюдением «Инструкции по работе в прикладном программном обеспечении»;

в) возможность восстановления данных в случае аварийного завершения работы программного обеспечения;

г) антивирусная защита:

Каждая рабочая станция должна автоматически проверяться на наличие вирусов при включении компьютера;

На каждой рабочей станции должна быть предусмотрена автоматическая проверка информации, поступающей через электронную почту, на наличие вирусов;

Каждая рабочая станция должна быть оснащена антивирусным программным обеспечением, способным обнаруживать и удалять найденные вирусы. Антивирусное программное обеспечение должно обновляться регулярно.

Системный администратор проводит профилактические работы по антивирусной защите в соответствии с «Регламентом информационной безопасности».

Специальные и профилактические мероприятия

а) В соответствии с «Регламентом информационной безопасности» системный администратор выполняет специальные работы по защите системной среды от изменений, а также проводит профилактические мероприятия для предотвращения сбоев в системной среде;

б) В соответствии с «Регламентом информационной безопасности» системный администратор выполняет специальные работы по защите локальной сети от несанкционированного доступа, а также проводит профилактические мероприятия для предотвращения сбоев в работе локальной сети;

в) В соответствии с «Регламентом информационной безопасности» администратор прикладной базы данных выполняет специальные работы по защите электронной базы данных, а также проводит профилактические мероприятия для предотвращения сбоев в работе прикладного программного обеспечения.

XI. Требования к техническому обеспечению Общества

51. В целях обеспечения информационной безопасности и защиты конфиденциальной информации необходимо соблюдать следующие требования к техническому обеспечению Общества:

а) Обеспечение соответствующего качества технического обеспечения Общества, гарантирующего непрерывную работу технических средств Общества на протяжении всего срока эксплуатации ресурса при необходимых условиях эксплуатации,

б) Достаточный объём памяти для хранения информации;

в) Соответствие ресурсов, достаточных для обработки информации;

г) Совместимость с другими техническими средствами, используемыми Обществом;

д) Строгое использование серверов, рабочих станций, сетевого оборудования, источников бесперебойного питания и других технических средств в соответствии с Порядком использования средств вычислительной техники и технического оборудования;

е) Обеспечение надлежащего состояния технических средств, своевременное проведение профилактических и ремонтных работ;

ж) Использование технических средств для аппаратной защиты конфиденциальной информации.

XII. Требования к контролю за защитой конфиденциальной информации

52. Ответственное подразделение Общества осуществляет регулярный контроль за соблюдением работниками Общества требований по защите конфиденциальной информации.

53. Ответственное подразделение Общества обязано:

а) Сообщать Директору Общества о выявленных нарушениях требований законодательства по обеспечению информационной безопасности (далее — нарушение правил);

б) Устанавливать причины совершения нарушения правил;

в) Осуществлять контроль за устранением выявленных нарушений правил.

Ответственный отдел Общества имеет следующими права:

а) вносить предложения по предотвращению выявленных нарушений правил;

б) вносить предложения о применении мер ответственности к нарушителям правил.

54. При осуществлении контроля за выполнением требований по защите конфиденциальной информации ответственное подразделение Общества должно обратить внимание на следующее:

а) на правильность оформления учетных данных документов, содержащих конфиденциальную информацию;

б) на наличие всех документов, содержащих конфиденциальную информацию, полученных и подготовленных сотрудниками;

в) наличие соответствующих оформляющих документов на конфиденциальные документы, которые отсутствуют (уничтожены, утеряны, признаны непригодными);

г) Порядок хранения и работы с документами, содержащими конфиденциальную информацию, на рабочих местах, а также другие вопросы.

55. В случае выявления нарушения правил со стороны сотрудников, ответственное подразделение Общества составляет акт о выявленном нарушении и направляет уведомление Директору Общества.

XIII. Ответственность лиц, допущенных к использованию конфиденциальной информации

56. По распоряжению Директора Общества ответственное подразделение Общества назначается ответственным за организацию и осуществление контроля за защитой конфиденциальной информации. Данное подразделение несёт ответственность за обеспечение надлежащего уровня контроля за соблюдением сотрудниками Общества требований по защите конфиденциальной информации.

57. Лица, обладающие конфиденциальной информацией, включая ответственного сотрудника, не имеют права использовать данную информацию в личных целях, а также передавать третьим лицам.

58. Лица, разгласившие конфиденциальную информацию без наличия соответствующего разрешения на использование, несут ответственность в соответствии с действующим законодательством.

XIV.Разглашение конфиденциальной информации

59. Разглашение конфиденциальной информации третьим лицам осуществляется в случаях и порядке, установленных законодательством.

60. Разглашение конфиденциальной информации третьим лицам осуществляется только на основании письменного запроса и с разрешения Директора Общества.

61. Запрос третьих лиц на получение конфиденциальной информации подлежит регистрации в журнале учета конфиденциальной информации Общества.

XV. Заключительные положения

62. Настоящая Инструкция вступает в силу после утверждения решением Наблюдательного совета Общества.

63. В настоящую Инструкцию могут быть внесены изменения и/или дополнения в связи с изменениями в законодательных актах, внесением изменений и/или дополнений в Устав Общества, а также в иных случаях.

64. Изменения и/или дополнения в настоящую Инструкцию вступают в силу после их утверждения решением Наблюдательного совета Общества.

65. В случае, если отдельные положения настоящей Инструкции противоречат действующему законодательству Республики Узбекистан и/или Уставу Общества, такие положения утрачивают силу, и до внесения соответствующих изменений в настоящую Инструкцию вопросы, регулируемые данными положениями, подлежат регулированию в соответствии с нормами действующего законодательства Республики Узбекистан и/или Уставом Общества.