«УТВЕРЖДЕНО»
Решением Наблюдательного совета
АО «O'ZSUVLOYIHA»
от «30» мая 2016 г.
(протокол б/н от «30» мая 2016 г.)

ИНСТРУКЦИЯ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АКЦИОНЕРНОГО ОБЩЕСТВА «O'ZSUVLOYIHA»

Ташкент – 2016г.

СОДЕРЖАНИЕ

I. ОБЩИЕ ПОЛОЖЕНИЯ

II. КРИТЕРИИ ОТНЕСЕНИЯ ИНФОРМАЦИИ К КАТЕГОРИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

III. ПОРЯДОК ВКЛЮЧЕНИЯ ИНФОРМАЦИИ, СОСТАВЛЯЮЩУЮ КОММЕРЧЕСКУЮ ТАЙНУ, СВЕДЕНИЙ, КОТОРЫЕ МОГУТ ПОВЛИЯТЬ НА ИЗМЕНЕНИЕ ЦЕНЫ ИНФОРМАЦИИ, А ТАКЖЕ ИНОЙ ИНФОРМАЦИИ ОБЩЕСТВА, К КОТОРОЙ ОГРАНИЧЕН ДОСТУП В ПЕРЕЧЕНЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

IV. ДОПУСК СОТРУДНИКОВ ОБЩЕСТВА И ИНЫХ ЛИЦ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

V. ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

VI. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

VII. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ ОБЩЕСТВА

VIII ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, ГДЕ РАСПОЛАГАЮТСЯ ТЕХНИЧЕСКИЕ СРЕДСТВА, ОБРАБАТЫВАЮЩИЕ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

IX. ТРЕБОВАНИЯ К ХРАНИЛИЩАМ, ГДЕ ОБЕСПЕЧИВАЕТСЯ НАДЛЕЖАЩЕЕ ХРАНЕНИЕ ДОКУМЕНТОВ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

X. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ОБЩЕСТВА

XI. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ ОБЩЕСТВА

XII. ТРЕБОВАНИЯ К КОНТРОЛЮ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

XIII. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ОБЩЕСТВА И ЧЛЕНОВ ОРГАНОВ УПРАВЛЕНИЯ И КОНТРОЛЯ ОБЩЕСТВА

XIV. РАСКРЫТИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

XV. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящяя Инструкция разработана в соответствии с «Положением об информационной политике Акционерного общества «O'ZSUVLOYIHA» (далее – Общество), а также «Положением об орагнизации защиты конфиденциальной информации эмитентами» (№2081 от 24.02.2010 г.) и определяет порядок отнесения информации к Перечню конфиденциальной информации, а также организации ее защиты.

2. В настоящем Положении используются следующие основные понятия:

- **конфиденциальная информация** - документированная информация, доступ к которой ограничивается в соответствии с законодательством;
- **коммерческая тайна** - информация, имеющая коммерческую ценность в научно-технической, технологической, производственной, финансово-экономической и других сферах в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и собственник этой информации принимает меры по защите ее конфиденциальности;
- **инсайдерская информация** – точная и конкретная информация, которая не была распространена или предоставлена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну), распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, товаров Общества.

II. КРИТЕРИИ ОТНЕСЕНИЯ ИНФОРМАЦИИ К КАТЕГОРИИ КОНФИДЕНЦИАЛЬНОЙ

2. К категории конфиденциальной информации относится коммеческая тайна, инсайдерская информация и иная информация, доступ к которой ограничен.

3. К коммерческой тайне относится информация, которая:

имеет действительную или потенциальную коммерческую ценность для Общества в силу неизвестности ее третьим лицам;

не обладает признаками государственных секретов и иной охраняемой законом тайны

не являться общеизвестной или общедоступной в соответствии с законодательством;

обеспечиваться мерами защиты ее конфиденциальности.

4. К инсайдерской информации относится информация, указанная в Приложении № 1 к настоящему Положению.

5. К иной информации Общества, к которой ограничен доступ, относится следующая информация:

I. Информация о производственной деятельности Общества, являющаяся коммерческой тайной Общества:

а) сведения о производственных мощностях Общества;

б) сведения о технологических процессах;

в) сведения о планах расширения или свертывания производства;

г) планы перспективного развития Общества;

д) разработки (ноу-хау) Общества;

е) сведения о продвижении на рынок новых видов продукции, товаров, работ и услуг;

ж) стратегия тарифной политики;

з) стратегия кадровой политики;

и) иная информация (определяется Обществом).

II. Информация о финансово-хозяйственной деятельности Общества:

а) сведения о хозяйственных договорах, заключаемых Обществом с поставщиками на закупку продукции, товаров, выполнение работ или оказание услуг;

б) сведения о хозяйственных договорах, заключаемых Обществом с потребителями на поставку продукции, товаров, выполнение работ и оказание услуг;

в) сведения о финансовых операциях Общества;

г) сведения о данных бухгалтерского учета и отчетности;

д) протоколы и отчеты Службы внутреннего аудита Общества;

е) акты проверок финансово-хозяйственной деятельности Общества государственными контролирующими органами;

ж) иная информация (определяется Обществом)..

III. Информация об Обществе как участнике рынка ценных бумаг:

а) сведения об акционерах Общества (персональные данные по физическим лицам и реквизиты по юридическим лицам, не являющиеся общедоступными);

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

в) сведения о типе и количестве принадлежащих владельцам ценных бумаг корпоративных облигаций Общества;

г) решения органов управления Общества до их раскрытия эмитентом в установленном законодательством порядке;

д) любые сведения о деятельности Общества как акционерного общества, не являющиеся общедоступными;

е) любая информация, предоставляемая акционерам Общества и не являющаяся общедоступной для иных лиц;

ж) реестры акционеров Общества;

з) реестры владельцев корпоративных облигаций Общества;

и) регистрационные списки участников общих собраний акционеров Общества;

к) протоколы Счетной комиссии, бюллетени для голосования;

л) приказы Генерального директора Общества;

м) протоколы заседаний Ревизионной комиссии Общества и выписки из протоколов;

н) заключения и отчеты аудитора Общества;

о) списки аффилированных лиц Общества;

п) ведомости начисления и выплаты дивидендов акционерам Общества;

р) ведомости начисления и выплаты процентов владельцам корпоративных облигаций Общества;

с) акты проверок деятельности Общества на рынке ценных бумаг уполномоченным государственным органом по регулированию рынка ценных бумаг;

т) иная информация (определяется Обществом)..

III. ПОРЯДОК ВКЛЮЧЕНИЯ ИНФОРМАЦИИ, КОММЕРЧЕСКОЙ ТАЙНЫ, А ТАКЖЕ СВЕДЕНИЙ, КОТОРЫЕ МОГУТ ПОВЛИЯТЬ НА ИЗМЕНЕНИЕ ЦЕНЫ АКЦИЙ В ПЕРЕЧЕНЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4. Информация, являющаяся коммерческой тайной, а также распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, товаров Общества включается в Перечень конфиденциальной информации (далее - Перечень) в порядке, установленным настоящим Положением.

5. Ведение Переченя осуществляется наименование отдела.

6. Для принятия решения о включении в Перечень конфиденциальной инфомации отделу (наименование отдела) представляется:

документ, подтверждающего действительную или потенциальную коммерческую ценность для ее Общества в силу неизвестности ее третьим лицам;

информация, что данная информация не является общеизвестной или общедоступной в соответствии с законодательством и требует обеспечения необходимыми мерами зашиты ее конфиденциальности.

7. Для рассмотрения представленной информации и принятия решения о включении той или иной информации в Перечень и исключения их из него в Обществе создается ответствующая Комиссия.

8. Состав Комиссии и регламент его работы утверждается Генеральным директором.

9. Комиссия в трехдневный срок рассматривает информацию и приложенные к ней материалы, представленные отделу (наименование отдела) в соответствии с пунктом 6 настоящего Положения, по результатам которого принимает решение о включении предприятия в Перечень.

10. Отделом (наименование отдела) на постоянной основе осуществляет мониторинг информации, включенной в Перечень.

11. В случае выявления по результатам мониторинга информации, не отвечающей ни одному из критериев, указанным в пункте 3 настоящего Положения, отделом (наименование отдела) совместно с Комиссией принимается решение об исключении ее из Перечня.

IV. ДОПУСК СОТРУДНИКОВ ОБЩЕСТВА И ИНЫХ ЛИЦ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

12. Допуск к конфиденциальной информации Общества имеют следующие лица:

а) лицо, осуществляющее функции единоличного исполнительного органа (Управляющая организация, временный единоличный исполнительный орган), а также коллегиального ;

б) члены Наблюдательного совета и Ревизионной комиссии Общества, получившие доступ к конфиденциальной информации для выполнения возложенных на них обязанностей по управлению Обществом;

в) лица, которые владеют не менее чем 25 процентами голосующих акций Общества;

г) лица, имеющие доступ к конфиденциальной информации Общества на основании договоров, заключенных с соответствующими лицами, в том числе аудиторы (аудиторские организации), оценщики (юридические лица, с которыми оценщики заключили трудовые договоры), профессиональные участники рынка ценных бумаг, кредитные организации, страховые организации;

д) лица, осуществляющие присвоение рейтингов Обществу, а также ценным бумагам Общества;

е) сотрудники, получившие допуск к конфиденциальной информации Общества в соответствии со своими должностными обязанностями, в том числе работники Службы внутреннего аудита Общества;

ж) иные лица в случаях и порядке, предусмотренных законодательством.

13. В целях учета лиц, имеющих доступ к конфиденциальной информации Общества должно быть организовано ведение Списка лиц, имеющих доступ к конфиденциальной информации Общества.

14. Структурным подразделением, ответственным за ведение Списка и осуществление контроля за обращением таковой информации, является Отдел (наименование отдела).

15.Выдача архивных документов, содержащих конфиденциальную информацию, осуществляется только на основании утвержденного приказом Генерального директора Общества списка лиц, имеющих допуск к архивным документам, содержащим конфиденциальную информацию.

16.Допуск лиц к конфиденциальной информации Общества предоставляется Генеральным директором Общества при соблюдении следующих условий:

а) оформление письменного обязательства о сохранении и неразглашении сотрудником сведений, составляющих конфиденциальную информацию;

б) ознакомление лиц с требованиями законодательства по обеспечению защиты конфиденциальной информации.

17.Сотрудники Общества могут получать допуск к сведениям, составляющим конфиденциальную информацию Общества, только в пределах своих должностных обязанностей и в объеме, действительно необходимом им для их выполнения.

18. Генеральный директор Общества несет персональную ответственность за правомерность выдачи сотрудникам допуска к сведениям, составляющим конфиденциальную

19. Лица, имеющие допуск к конфиденциальной информации, обязаны:

а) строго хранить в тайне сведения, отнесенные к конфиденциальной информации;

б) выполнять требования законодательства по обеспечению защиты конфиденциальной информации;

в) работать только с теми сведениями и документами, содержащими конфиденциальную информацию, к которым получили доступ;

г) не использовать конфиденциальную информацию в личных целях;

д) незамедлительно сообщать своему непосредственному начальнику или Генеральному директору Общества о попытках посторонних лиц получить от сотрудников конфиденциальную информацию, об утрате или недостаче бумажных и электронных носителей конфиденциальной информации, ключей от помещений, хранилищ, сейфов, где находятся документы, содержащие конфиденциальную информацию, и о других фактах, которые могут привести к разглашению конфиденциальной информации, а также о причинах и условиях утечки конфиденциальной информации;

е) в случае прекращения отношений лицом, в силу которых данное лицо имело доступ к конфиденциальной информации (увольнения) передать все бумажные и электронные носители конфиденциальной информации, которые находились в его распоряжении в связи с выполнением им функциональных обязанностей своему непосредственному начальнику или Генеральному директору Общества.

ж) сотрудники могут нести и иные обязанности в соответствии с законодательством.

20. Лицо подлежит исключению из Списка Общества в день, следующий за днем, когда Общество узнало о прекращении отношений с лицом, в силу которых данное лицо имело доступ к конфиденциальной информации.

21. Генеральный директор Общества должен принимать необходимые меры по исключению возможности ознакомления с конфиденциальной информацией сотрудников, которым она не требуется при выполнении ими своих должностных обязанностей.

V. ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

22. Общество принимает необходимые меры по обеспечению защиты конфиденциальной информации в соответствии с законодательством.

23. Защита конфиденциальной информации Обществом осуществляется

в целях предотвращения утечки, хищения, утраты, искажения, блокировки, подделки конфиденциальной информации и иного несанкционированного доступа к ней, а также предотвращения несанкционированных действий по уничтожению, блокированию, копированию, искажению конфиденциальной информации и других форм вмешательства в информационные ресурсы и информационные системы Общества.

24. Организация и осуществление контроля за обеспечением защиты конфиденциальной информации возлагается на ответственного сотрудника Общества, назначаемого Генеральным директором Общества (далее – ответственный сотрудник Общества).

25. Организация защиты конфиденциальной информации Общества осуществляется путем соблюдения следующих требований:

а) составление и утверждение перечня конфиденциальной информации Общества, ознакомление каждого сотрудника Общества с перечнем конфиденциальной информации Общества и подписание им обязательства о неразглашении конфиденциальной информации, предусмотрение во внутренних документах Общества, в трудовых договорах и должностных инструкциях сотрудников Общества ответственности за разглашение конфиденциальной информации Общества;

б) разграничение доступа к конфиденциальной информации;

в) требования к порядку учета, хранения и работы с конфиденциальной информацией;

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

д) требования к помещениям, где располагаются технические средства, обрабатывающие конфиденциальную информацию;

е) требования к хранилищам, где обеспечивается надлежащее хранение документов, содержащих конфиденциальную информацию;

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

з) требования к программному обеспечению Общества;

и) требования к контролю за обеспечением защиты конфиденциальной информации Общества;

к) требования по раскрытию конфиденциальной информации Общества.

VI. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

26. Конфиденциальная информация Общества может содержаться в документах текущего периода и в архивных документах.

Конфиденциальная информация может содержаться на бумажных и электронных носителях (электронные документы, копии баз данных, текстовые, табличные и графические файлы, содержащие конфиденциальную информацию).

27. Учет, хранение и работа с документами текущего периода, содержащими конфиденциальную информацию, осуществляется в структурных подразделениях Общества в соответствии с внутренними регламентами.

Учет архивных документов, содержащих конфиденциальную информацию, ведется в соответствующих журналах в бумажном и (или) электронном видах.

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

28. Документы Общества, содержащую конфиденциальную информацию, сдаются в Архив Общества не позднее 3 (трех) месяцев после завершения очередного финансового года.

29. Архивные документы, содержащие конфиденциальную информацию, должны храниться в помещении Архива Общества в металлических шкафах и (или) сейфах, которые должны иметь прочные засовы и во внерабочее время опечатываться (пломбироваться).

30. Запрещается хранить архивные документы, содержащие конфиденциальную информацию, в местах, не предназначенных для хранения подобного рода документов.

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

32. Отправка документа, содержащего конфиденциальную информацию, по почте осуществляется в порядке, предусмотренном законодательством.

33. Факт ознакомления с архивными документами, содержащими конфиденциальную информацию, подлежит оформлению на карточке учета выдаваемых архивных документов (дел), содержащих конфиденциальную информацию, и в журнале учета документов, содержащих конфиденциальную информацию, по форме согласно приложениям № 2 и № 3 к настоящей Инструкции.

34. Размножение, копирование, тиражирование либо раскрытие содержания документа, содержащего конфиденциальную информацию, осуществляется только в случаях, предусмотренных законодательством, на основании письменного разрешения Генерального директора Общества.

35. Отобранные к уничтожению документы, содержащие конфиденциальную информацию, перед сдачей на переработку в качестве макулатуры должны измельчаться до степени, исключающей возможность прочтения текста, или должны быть сожжены в специально отведенном месте.

36. После уничтожения документов, содержащих конфиденциальную информацию, в журнале учета проставляется соответствующая отметка.

37. Эмитент должен предпринимать необходимые меры для обеспечения защиты конфиденциальной информации от утечки и несанкционированного доступа при использовании информационно-коммуникационных технологий (далее - ИКТ).

38. Доступ в помещения, где размещены ИКТ и базы данных, обрабатывающие конфиденциальную информацию, разрешается только лицам, имеющим соответствующий допуск.

39. Лица, эксплуатирующие и обслуживающие ИКТ, обязаны:

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

б) соблюдать установленный режим разграничения доступа к конфиденциальной информации;

в) незамедлительно информировать своего непосредственного начальника или Генерального директора Общества обо всех фактах попыток несанкционированного доступа к конфиденциальной информации, утечки или порчи такой информации.

40. Подключение ИКТ к сетям общего пользования должно осуществляться исключительно при наличии производственной необходимости и только с применением средств защиты информации.

41. При выходе из строя или списании ИКТ, обрабатывавших конфиденциальную информацию, необходимо предпринимать меры по полному уничтожению содержащейся в них информации для недопущения ее восстановления.

VII. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ ОБЩЕСТВА

42. При работе с конфиденциальной информацией на бумажных и электронных носителях в структурных подразделениях Общества сотрудники Общества должны обеспечить её сохранность и учет.

43. К структурным подразделениям Общества, которые используют в работе конфиденциальную информацию, предъявляются следующие требования:

а) хранение документов, содержащих конфиденциальную информацию в специально отведенных для этих целей металлических шкафах и/или сейфах;

б) соблюдение внутренних регламентов по работе с документами, содержащими конфиденциальную информацию;

в) бумажные документы, находящиеся на рабочих столах сотрудников Общества, не должны быть доступны для обозрения посторонними лицами;

г) недопущение оставления документов, содержащих конфиденциальную информацию без присмотра при оставлении рабочего места (обеденный перерыв, рабочий перерыв, уход с работы);

д) при выходе работников из помещения бумажные документы помещаются в закрывающийся ящик рабочего стола, после окончания рабочего дня помещаются на хранение в закрывающиеся металлические шкафы и/или сейфы в помещении соответствующего структурного подразделения Общества;

е) копирование и модификация бумажных документов осуществляется строго в соответствии с внутренними регламентами Общества, ведется регистрация и учет копирования и модификации;

ж) уничтожение бумажных документов осуществляется строго в соответствии с внутренними регламентами;

з) контроль начальником структурного подразделения за соблюдением своими сотрудниками требований, установленных в Обществе применительно допуска к документам, содержащим конфиденциальную информацию.

VIII. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, ГДЕ РАСПОЛАГАЮТСЯ ТЕХНИЧЕСКИЕ СРЕДСТВА, ОБРАБАТЫВАЮЩИЕ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ.

44. Общество должно составить список помещений, где располагаются технические средства, обрабатывающие конфиденциальную информацию Общества (производственные помещения, бухгалтерия, юридическая служба, кабинет отдела корпоративных отношений с акционерами и другие структурные подразделения Общества).

45. К помещениям, где располагаются технические средства, обрабатывающие конфиденциальную информацию Общества, предъявляются следующие требования:

а) установка запираемых на замок металлических дверей в данных помещениях;

б) оснащение помещений средствами охранной и пожарной сигнализации;

в) соблюдение в данных помещениях соответствующего режима работы технических средств, обрабатывающих конфиденциальную информацию (температура, уровень влажности и другие требования, предусмотренные условиями эксплуатации технических средств);

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

д) наличие защитных мер по предотвращению несанкционированного подключения к техническим средствам, обрабатывающим конфиденциальную информацию.

IX. ТРЕБОВАНИЯ К ХРАНИЛИЩАМ, ГДЕ ОБЕСПЕЧИВАЕТСЯ НАДЛЕЖАЩЕЕ ХРАНЕНИЕ ДОКУМЕНТОВ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ.

46. Документы Общества, содержащие конфиденциальную информацию, должны храниться в специально предназначенном для этого хранилище – в Архиве Общества, где хранятся другие архивные документы по деятельности Общества.

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

48. К Архиву Общества предъявляются следующие требования:

а) установка запираемых на замок металлических дверей в помещении Архива Общества;

б) металлические решетки на окнах;

в) оснащение помещений Архива средствами охранной и пожарной сигнализации;

г) соблюдение в данных помещениях соответствующего режима хранения документов (температура, уровень влажности и другие требования, предусмотренные условиями надлежащего хранения);

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

е) наличие отдельного сейфа для хранения страховочных копий особо ценных документов Общества;

ж) ограничение свободного входа посетителей и посторонних лиц в помещение Архива.

X. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ОБЩЕСТВА.

49. Для обеспечения информационной безопасности и защиты конфиденциальной информации необходимо соблюдение следующих

требований к программному обеспечению Общества (системному, сетевому и прикладному):

а) соответствующее системное программное обеспечение, поддерживающее работоспособность системной среды (операционной системы серверов и рабочих станций и пр.);

б) соответствующее сетевое программное обеспечение, поддерживающее работоспособность локальной сети Общества;

в) соответствующее прикладное программное обеспечение, поддерживающее работоспособность прикладного программного обеспечения;

г) наличие соответствующей документации к прикладному программному обеспечению;

д) возможность разграничения уровня доступа пользователям прикладного программного обеспечения;

е) возможность резервного копирования прикладных баз данных;

ж) надлежащее хранение и учет прикладных баз данных;

з) защита информации от утери, порчи, разрушения, несанкционированного доступа посторонних лиц;

и) наличие процедур по восстановлению информации.

50. При работе с конфиденциальной информацией на электронных носителях ее защита обеспечивается следующими мерами:

а) запрет на несанкционированный доступ к информации;

б) защита от несанкционированного копирования, модификации и уничтожения;

в) защита информации от утери и разрушения;

г) специальные и профилактические работы.

Защита электронной информации от несанкционированного доступа:

а) пароль на включение компьютера;

Каждая рабочая станция (компьютер пользователя) должна быть защищена паролем на включение (на вход). Сотрудники Общества не должны сообщать пароль для ввода другим лицам.

б) разграничение доступа к сетевым ресурсам;

Доступ к сетевым ресурсам устанавливает Сетевой администратор в соответствии с должностными обязанностями сотрудников на основании рапорта начальника структурного подразделения Общества.

в) разграничение доступа к функциям прикладного программного обеспечения и базам данных;

Доступ к функциям прикладного программного обеспечения и базам данных устанавливает Администратор прикладных баз в соответствии с должностными обязанностями сотрудников Общества.

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

д) шифрование и защита паролем отдельных файлов с конфиденциальной информацией.

Защита электронной информации от несанкционированного копирования, модификации и уничтожения:

а) специальная защита файлов на возможность копирования, модификации и уничтожения;

б) копирование и модификация электронной информации только в соответствии с Порядком копирования конфиденциальной информации;

в) уничтожение электронной информации только в соответствии с Порядком уничтожения документов, содержащих конфиденциальную информацию.

Защита электронной информации от утери и разрушения:

а) эксплуатация серверов, рабочих станций, сетевого оборудования и других технических средств строго в соответствии с Порядком эксплуатации средств вычислительной техники и технического оборудования;

б) выполнение работ в электронных базах данных строго в соответствии с Инструкцией по работе в прикладном программном обеспечении;

в) возможность восстановления данных при аварийных завершениях работы программ;

г) антивирусная защита:

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

При поступлении информации из электронной почты на каждой рабочей станции должна быть предусмотрена автоматическая проверка на наличие вирусов;

Каждая рабочая станция должна быть оснащена антивирусным программным обеспечением, позволяющим удалять обнаруженные вирусы. Антивирусное программное обеспечение должно регулярно обновляться;

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

Специальные и профилактические работы.

а) выполнение Системным администратором в соответствии Регламентом информационной безопасности специальных работ для защиты системной среды от изменений и профилактических работ для предотвращения разрушения системной среды;

б) выполнение Сетевым администратором в соответствии с Регламентом информационной безопасности специальных работ для защиты локальной сети от несанкционированного доступа и профилактических работ для предотвращения сбоев в работе локальной сети;

в) выполнение специальных работ Администратором прикладных баз данных в соответствии с Регламентом информационной безопасности для защиты электронных баз данных и профилактических работ для предотвращения сбоев в работе прикладного программного обеспечения.

XI. Требования к техническому обеспечению Общества.

51. Для обеспечения информационной безопасности и защиты конфиденциальной информации необходимо соблюдение следующих требований к техническому обеспечению Общества:

а) соответствующее качество технического обеспечения Общества, обеспечивающего его бесперебойную работу в условиях надлежащей эксплуатации в течение всего срока до выработки ресурса;

б) емкость памяти, достаточная для хранения информации;

в) производительность ресурсов, достаточная для обработки информации;

г) совместимость с другими средствами технического обеспечения, используемыми Обществом;

д) эксплуатация серверов, рабочих станций, сетевого оборудования, источников бесперебойного питания и других технических средств строго в соответствии с Порядком эксплуатации средств вычислительной техники и технического оборудования;

е) поддержание в надлежащем рабочем состоянии технических средств, своевременное проведение профилактических и ремонтных работ;

ж) применение технических средств по аппаратной защите конфиденциальной информации.

XII. Требования к контролю по защите конфиденциальной информации.

52. Ответственный сотрудник Общества регулярно осуществляет контроль над выполнением сотрудниками Общества требований по защите конфиденциальной информации.

53. Ответственный сотрудник Общества обязан:

а) незамедлительно сообщать Генеральному директору Общества о выявленном нарушении требований законодательства по обеспечению защиты конфиденциальной информации (далее — нарушение);

б) устанавливать причины совершения нарушения;

в) контролировать устранение выявленных нарушений;

Ответственный сотрудник Общества имеет право:

а) вносить предложения по недопущению впредь выявленных нарушений;

б) вносить предложения о применении к нарушителям мер ответственности.

54. При осуществлении контроля за обеспечением защиты конфиденциальной информации ответственному сотруднику Общества следует обращать внимание на следующее:

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

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

в) наличие соответствующих документов на отсутствующие (уничтоженные, утерянные, поврежденные и т. д.) документы, содержащие конфиденциальную информацию;

г) соблюдение порядка хранения и работы с документами, содержащими конфиденциальную информацию, на рабочих местах, а также на иные вопросы.

55. При выявлении допущенных сотрудниками нарушений ответственный сотрудник Общества составляет акт о выявленном нарушении и представляет рапорт Генеральному директору Общества.

XII. Ответственность лиц, имеющих доступ к конфиденциальной информации.

56. Ответственный сотрудник Общества, на которого приказом Генерального директора Общества возлагается организация и осуществление контроля за обеспечением защиты конфиденциальной информации, несет ответственность за ненадлежащее осуществление контроля за выполнением сотрудниками Общества требований по защите конфиденциальной информации.

57. Лица, указанные в п.19, располагающие конфиденциальной информацией, в том числе ответственный сотрудник не вправе использовать эту информацию в личных целях, а также передавать ее третьим лицам.

За разглашение конфиденциальной информации лица, имеющие доступ к такой информации, несут ответственность в порядке, установленном законодательством.

XIII. Раскрытие конфиденциальной информации.

58. Раскрытие конфиденциальной информации третьим лицам осуществляется в случаях и порядке, предусмотренном законодательством.

59. Раскрытие конфиденциальной информации третьим лицам осуществляется только на основании письменного запроса и разрешения Генерального директора Общества.

60. Запросы от третьих лиц на получение конфиденциальной информации фиксируются в Журнале учета конфиденциальной информации Общества.

XIV. Заключительные положения.

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

62. В настоящую Инструкцию могут быть внесены изменения и/или дополнения в связи с изменением законодательства, внесения изменений и/или дополнений в Устав Общества и других случаях.

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

64. Если отдельные статьи настоящей Инструкции вступают в противоречие с действующим законодательством Республики Узбекистан и/или Уставом Общества, эти статьи утрачивают силу и в части регулируемых этими статьями вопросов следует руководствоваться нормами действующего законодательства Республики Узбекистан и/или Устава Общества до момента внесения соответствующих изменений в настоящую Инструкцию.

Генеральный директор
АО “O'ZSUVLOYIHA” **М. Наджимов**