Муниципальное образование
«Токсовское городское поселение»
Всеволожского муниципального района Ленинградской области

АДМИНИСТРАЦИЯ

ПОСТАНОВЛЕНИЕ

28.04.2017 № 94

г.п. Токсово

Об утверждении Положения о порядке организации и проведения работ по защите конфиденциальной информации в администрации МО «Токсовское городское поселение» Всеволожского муниципального района Ленинградской области и подведомственных ей муниципальных предприятиях и учреждениях

В соответствии с Конституцией РФ, Трудовым кодексом РФ от 30декабря 2001 года N 197-ФЗ, Федеральным законом РФ от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом РФ от 27 июля 2006 года N 152-ФЗ "О персональных данных", Указом Президента РФ от 6 марта 1997 года N 188 "Об утверждении перечня сведений конфиденциального характера", с целью определения порядка обработки персональных данных в администрации МО «Токсовское городское поселение»,

ПОСТАНОВЛЯЮ:

1. Утвердить Положение о порядке организации и проведения работ по защите конфиденциальной информации в администрации МО «Токсовское городское поселение» Всеволожского муниципального района Ленинградской области и подведомственных ей муниципальных предприятиях и учреждениях.
2. Специалисту 1-ой категории сектора по связям с общественностью и социальной работе Сигаевой С.Ю. ознакомить всех работников администрации МО «Токсовское городское поселение» с настоящим постановлением под роспись.
3. Настоящее Постановление подлежит официальному опубликованию в газете «Вести Токсово», размещению на официальном сайте МО «Токсовское городское поселение» http://www.toksovo-lo.ru в сети Интернет.
4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава администрации А.С. Кожевников

Заказ №252 от 18.08.2016г. Тираж 500 экз.

УТВЕРЖДЕНО
постановлением главы администрации
МО «Токсовское городское поселение»
от 28. 04. 2017 г. № 94

Положение
о порядке организации и проведения работ по защите конфиденциальной информации в администрации МО «Токсовское городское поселение» Всеволожского муниципального района Ленинградской области и подведомственных ей муниципальных предприятиях и учреждениях

1. Общие положения

Настоящее Положение о порядке организации и проведения работ по защите конфиденциальной информации (далее «Положение») определяет общий порядок обращения с конфиденциальной информацией в администрации МО «Токсовское городское поселение» (далее – «Администрация»), а также в подведомственных ей муниципальных предприятиях и учреждениях (далее – «муниципальные учреждения») с целью соблюдения надлежащих правил обращения с не содержащими государственной тайны конфиденциальными и другими защищаемыми сведениями, а также защиты прав и интересов Администрации и муниципальных учреждений в случае неправомерного обращения с защищаемой информацией.

Мероприятия по защите конфиденциальной информации, проводимые в Администрации и муниципальных учреждениях, являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

Положение также определяет порядок организации доступа пользователей к информационным ресурсам ограниченного доступа.

Целью настоящего Положения является:

-укрепление механизмов правового регулирования отношений в области защиты конфиденциальной информации;

-создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых.

Настоящее Положение основывается на Конституции Российской Федерации, Федеральном законе от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», «Специальных требованиях и рекомендациях по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России (ФСТЭК России) от 30 августа 2002 года №282, а также ряде иных нормативных правовых актов в сфере защиты конфиденциальной информации.

Действие Положения не распространяется на автоматизированные информационные системы хранения и обработки информации, содержащей сведения, составляющие государственную тайну.

Объектами защиты в Администрации МО «Токсовское городское поселение» Всеволожского муниципального района Ленинградской области являются:

- средства и системы информатизации и связи (средства вычислительной техники, средства, системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация - далее вспомогательные технические средства и системы (ВТСС);
- помещения (служебные кабинеты), специально предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения (далее – «ЗП»).

2. Понятие и состав конфиденциальной информации

2.1. В соответствии с Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера», к сведениям конфиденциального характера относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 года № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом

Российской Федерации и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

- сведения о сущности изобретения, полезной модели или Промышленного образца до официальной публикации информации о них.

Служебная предметная информация, составляющая служебную тайну, должна защищаться в соответствии с требованиями федерального законодательства, руководящих документов ФСБ России, ФСТЭК России, «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России (ФСТЭК России) от 30 августа 2002 года №282.

Обеспечение защиты персональных данных должно обеспечиваться в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и руководящих документов ФСТЭК России.

3. Информационные ресурсы, подлежащие защите

3.1. Информационные системы включают:

-государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

-муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

- иные информационные системы.

Оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении. Особенности эксплуатации муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами Администрации, принимающей решение о создании такой информационной системы.

Муниципальная информационная система создается в целях реализации полномочий органов местного самоуправления и обеспечения

обмена информацией между органами местного самоуправления (муниципальными учреждениями), а также в иных установленных муниципальными правовыми актами целях.

Технические средства, предназначенные для обработки информации, содержащейся в муниципальной информационной системе, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

Информация, содержащаяся в муниципальной информационной системе, а также иные имеющиеся в распоряжении Администрации (муниципальных учреждений) сведения и документы являются муниципальными информационными ресурсами. Информация, содержащаяся в муниципальных информационных системах, является официальной.

Администрация (муниципальные учреждения), в соответствии с нормативным правовым актом, регламентирующим функционирование муниципальной информационной системы, обязана(ы) обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» или другими федеральными законами.

3.2. Информационные ресурсы, содержащие конфиденциальную информацию, сформированные в процессе деятельности Администрации (муниципальных учреждений), а также приобретенные ей в муниципальную собственность установленными законодательством Российской Федерации, Ленинградской области, способами, являются муниципальной собственностью МО «Токсовское городское поселение» и не могут быть использованы иначе как с разрешения собственника или в установленных законом случаях.

3.3. Отнесение информации к конфиденциальной осуществляется обладателем такой информации в порядке, установленном законодательством Российской Федерации.

Перечень сведений конфиденциального характера Администрации (муниципальных учреждений), неправильное обращение с которыми может нанести ущерб их собственнику, владельцу или иному лицу, определяется главой администрации (руководителем муниципального учреждения) на основании предоставленных действующим законодательством прав.

Указанный перечень должен быть документально оформлен в виде Перечня сведений конфиденциального характера (далее – «Перечень»).

Для определения конфиденциальности сведений предлагается

использовать сводный перечень сведений конфиденциального характера, составленный в соответствии с нормативными правовыми актами (Приложение №1 к настоящему Положению), который должен утверждаться Администрацией (муниципальным учреждением) индивидуально.

Перечень сведений конфиденциального характера разрабатывается в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера», постановлением Правительства Российской Федерации от 5 декабря 1991 года №35 «О перечне сведений, которые не могут составлять коммерческую тайну», постановлением Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» и другими правовыми актами, определяющими состав сведений ограниченного распространения.

Информация конфиденциального характера не может быть использована в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан.

3.4. Администрация (муниципальные учреждения) как собственники (владельцы) информационных ресурсов, в соответствии с предоставленными им действующим законодательством правами и обязанностями, обязаны осуществлять учет ресурсов и устанавливать режим их защиты (комплексную систему защиты конфиденциальной информации).

Ответственность за организацию работ по установлению режима защиты конфиденциальной информации, правил ее обработки, разграничения допуска персонала и передачи (предоставления) третьим лицам возлагается на главу администрации (руководителей муниципальных учреждений).

Конфиденциальные (коммерческие и др.) сведения других юридических или физических лиц, переданные в Администрацию (муниципальные учреждения) для выполнения работ или осуществления иной совместной деятельности и в отношении которых Администрация (муниципальные учреждения) взяла на себя обязательство о неразглашении и исключении неправомерного их использования, подлежат защите наравне с другими сведениями, составляющими служебную тайну.

В случае ликвидации муниципального учреждения решение о дальнейшем использовании информации конфиденциального характера принимает Администрация.

4. Обязанности должностных лиц по защите конфиденциальной информации

4.1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования,

предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

- своевременное обнаружение фактов несанкционированного доступа к информации;

- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

- постоянный контроль за обеспечением уровня защищенности информации.

4.2. Должностные лица Администрации (муниципальных учреждений) обязаны принимать меры по защите информации конфиденциального характера.

Глава Администрации (руководитель муниципального учреждения) в пределах своей компетенции определяет:

- перечень сведений (информационных ресурсов), составляющих конфиденциальную информацию;

- порядок подготовки, учета и хранения документов и электронных носителей с конфиденциальной информацией;

- порядок обработки конфиденциальной информации с помощью средств вычислительной техники, аттестованных по требованиям безопасности информации организациями-лицензиатами ФСТЭК России;

- порядок передачи информации конфиденциального характера другим муниципальным учреждениям, а также между структурными подразделениями;

- порядок создания защищенных каналов связи при использовании международной сети Интернет. Для передачи служебной информации ограниченного распространения по линиям связи, выходящим за пределы контролируемой зоны Администрации (муниципального учреждения), необходимо использовать защищенные каналы связи. Применяемые технические средства защиты информации и программное обеспечение должны быть сертифицированы по требованиям безопасности информации;

- перечень защищаемых помещений Администрации (муниципального учреждения), предназначенных для проведения конфиденциальных мероприятий, и порядок защиты циркулирующей речевой конфиденциальной информации в данных помещениях, в системах

звукоусиления, при осуществлении ее магнитной звукозаписи и передачи по каналам связи.

5. Организационные и технические мероприятия по технической защите конфиденциальной информации

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются отдельными лицами, назначаемыми главой в Администрации для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.3. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на главу Администрации.

5.4. Техническая защита информации в защищаемых помещениях.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

- определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки);
- назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП, далее сотрудники, ответственные за безопасность информации;
- разработка частных инструкций по обеспечению безопасности информации в ЗП;
- обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения;
- инструктирование сотрудников, работающих в ЗП о правилах эксплуатации персональных электронно-вычислительных машин (ПЭВМ), других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации;
- проведение в ЗП обязательных визуальных проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП;
- исключение неконтролируемого доступа к линиям связи;
- осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах;
- обеспечение требуемого уровня звукоизоляции входных дверей и окон;

- демонтирование или заземление (с обеих сторон) лишних (незадействованных) проводников и кабелей;
- отключение при проведении совещаний всех неиспользуемых электро и радиоприборов от сетей питания и трансляции;
- выполнение перед проведением совещаний следующих условий:
  - окна должны быть плотно закрыты и зашторены;
  - двери плотно прикрыты.

Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.

При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.

Техническая защита информации в средствах вычислительной техники (СВТ) от несанкционированного доступа должна обеспечиваться путем выполнения необходимых организационных мер защиты, установки сертифицированных программных и аппаратно-технических средств защиты информации от несанкционированного доступа (далее – «НСД»), защиты каналов связи, предназначенных для передачи конфиденциальной информации, защиты информации от воздействия программ-закладок и компьютерных вирусов.

Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

- установки и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

Организация работ по антивирусной защите информации возлагается на руководителей структурных подразделений и должностных лиц, осуществляющих контроль за антивирусной защитой, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на специалиста по обслуживанию вычислительной техники.

Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;
- периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых

в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

К использованию допускается только лицензированные, сертифицированные антивирусные средства.

Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

- входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения;
- входной антивирусный контроль всей информации поступающей с электронной почтой;
- входной антивирусный контроль всей поступающей информации из сети Интернет;
- выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;
- периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;
- обязательная антивирусная проверка используемых в работе внешних носителей информации;
- обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;
- внеплановая антивирусная проверка внешних носителей и жестких дисков на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;
- восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных. О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов. При

обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на автоматизированном рабочем мечта (далее - «АРМ»), принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения компьютеров, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на ответственного специалиста.

Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

– длина пароля должна быть не менее восьми (8) символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести (6) позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Формирование личных паролей пользователей осуществляется централизованно. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

Полная плановая смена паролей пользователей должна проводиться регулярно.

Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

Периодический контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены и использования возлагается на ответственного сотрудника.

6. Порядок обращения с документами и электронными носителями информации, содержащими информацию конфиденциального характера

6.1. Конфиденциальная информация, содержащаяся в документах, имеющих обращение в Администрации (муниципальных учреждениях), является служебной информацией ограниченного распространения и составляет служебную тайну.

Требования по организации защиты служебной тайны установлены постановлением Правительства Российской Федерации от 3 ноября 1994 года №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».

На документах ограниченного распространения, содержащих конфиденциальную информацию, в необходимых случаях проставляется пометка «Для служебного пользования» (далее – «ДСП»).

Необходимость проставления пометки «Для служебного пользования» определяется исполнителем или должностным лицом, утверждающим документ.

Для обработки (в том числе и размножения) документов со служебной информацией ограниченного распространения используются только сертифицированные, аттестованные по требованиям безопасности информации технические средства её обработки, передачи и хранения.

При работе с документами с пометкой «ДСП» запрещается:

- публиковать сведения ограниченного распространения в средствах массовой информации;
- передавать по незащищённым каналам связи, в том числе локальным сетям, имеющим выход в сеть Интернет;
- передавать (принимать) документы без расписки должностного лица;
- пересылать сторонним организациям неустановленным порядком (документы с пометкой «ДСП» пересылаются фельдъегерской связью, заказным или ценным почтовым отправлением);
- копировать без письменного разрешения руководителя органа власти области, муниципального органа власти, муниципального учреждения разработавшего документ;
- хранить не в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах);
- передавать документы и дела с пометкой «ДСП» от одного муниципального служащего либо работника Администрации, работника муниципального учреждения, замещающего должность, не являющуюся должностью муниципальной службы, другому без письменного предписания соответствующего руководителя.

По фактам утраты документов (дел, изданий), содержащих служебную информацию ограниченного распространения, либо разглашения этой информации, главой Администрации (руководителем муниципального учреждения) создается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются главе Администрации (руководителю муниципального учреждения), создавшему комиссию.

6.2. На съемных электронных носителях информации (дискетах, магнитооптических дисках и т.д.), содержащих электронные документы конфиденциального характера, проставляется пометка «ДСП».

Учет (регистрация) отпечатанных с помощью средств вычислительной техники документов, содержащих информацию конфиденциального характера, осуществляется в порядке, определенном для бумажных носителей информации ограниченного доступа.

Электронные носители, содержащие конфиденциальную информацию, учитываются, как правило, структурными подразделениями (делопроизводителями) Администрации (муниципального учреждения), которым поручен прием и учет документированной служебной информации ограниченного пользования по журналу учета машинных носителей информации. Учетные реквизиты (регистрационный номер, пометка «ДСП», дата регистрации и подпись муниципального служащего либо работника Администрации, работника муниципального учреждения, замещающего должность, не являющуюся должностью муниципальной службы, отвечающего за учет носителей) проставляются на электронных носителях информации в удобном для просмотра месте.

6.3. Машинные носители информации с пометкой «ДСП»:

- регистрируются в подразделении, которому поручен учет документов с пометкой «ДСП», с проставлением учетных реквизитов;
- передаются другим исполнителям под подпись в журнале учета машинных носителей информации или по карточке учета;
- уничтожаются по акту.

6.4. Порядок рассылки, уничтожения, передачи, проверки наличия электронных носителей информации, проведения расследований по фактам утраты электронных носителей информации, снятия пометки «ДСП» с электронных носителей информации является таким же, как и для бумажных документов конфиденциального характера.

7. Организация работ по защите конфиденциальной информации при обработке на средствах вычислительной техники и при передаче по каналам в сети Интернет

Настоящий раздел Положения устанавливает требования к организации работ при обработке конфиденциальной информации с помощью средств вычислительной техники (далее – «СВТ»), в том числе при взаимодействии абонентов с информационными сетями общего пользования Интернет.

7.1. Лица, осуществляющие обработку информации ограниченного распространения на средствах вычислительной техники, несут ответственность за соблюдение ими порядка обращения с информацией и

обеспечения технической защиты конфиденциальной информации.

Режим защиты конфиденциальной информации (система защиты конфиденциальной информации) устанавливается собственником информационных ресурсов или уполномоченным лицом Администрации (муниципального учреждения) в соответствии с законодательством Российской Федерации, Ленинградской области, Всеволожского района и должен включать в себя:

- создание подразделения, назначение ответственных за обеспечение безопасности информации, формулирование должностных обязанностей работников и органов по организации защиты (охране) сведений конфиденциального характера (постановление Правительства Российской Федерации от 15 сентября 1993 года № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации»);

- определение обязанностей, ответственности за разглашение и ограничений, накладываемых на муниципального служащего района либо работника Администрации, работникам муниципального учреждения, замещающего должность, не являющуюся должностью муниципальной службы, допущенных к конфиденциальной информации;

- инвентаризацию и регистрацию информационных ресурсов, содержащих сведения конфиденциального характера;

- реализацию правил разграничения доступа к информации, составляющей конфиденциальные сведения, путем установления порядка и условий обращения (обмена) с этой информацией и контроля за соблюдением такого порядка (охраны ее конфиденциальности);

- учет лиц, получивших доступ к конфиденциальной информации;

- формулирование требований и организацию делопроизводства конфиденциальной информации;

- выявление, учет систем и средств информатизации, предназначенных (использующихся) для передачи, хранения, обработки и распространения конфиденциальной информации;

- разработку организационно-распорядительных документов по организации защиты информации:

- перечень сведений, составляющих конфиденциальную информацию Администрации (муниципального учреждения);

- создание системы разграничения доступа персонала к СВТ и информационным ресурсам;

- частные инструкции, регламентирующие порядок создания, учёта, хранения и уничтожения документированной информации ограниченного распространения Администрации (муниципального учреждения), а также порядок предотвращения несанкционированного доступа и защиты информации, обрабатываемой на СВТ;

- инструкции администратору информационной безопасности автоматизированной системы (далее – «АС»), пользователю;

- обеспечение технической защиты конфиденциальной информации (аттестация по требованиям безопасности информации средств и систем информатизации организациями-лицензиатами ФСТЭК России, использование сертифицированных технических средств обработки, передачи и хранения информации, а также средств и программно-аппаратных комплексов защиты информации, включая криптографические

средства);

- организацию контроля за реализацией выбранных мер защиты и за обеспечением конфиденциальности работ и информации.

7.2. Обеспечение защиты конфиденциальной информации при обработке ее на средствах вычислительной техники в Администрации (муниципальных учреждениях) осуществляется в соответствии с требованиями указанными в сборнике руководящих документов Гостехкомиссии России (ФСТЭК) по защите информации от несанкционированного доступа и «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР- К)», утвержденными приказом Гостехкомиссии (ФСТЭК) России от 30 августа 2002 года №282.

В Администрации (муниципальных учреждениях) разрабатывается частная инструкция по защите информации, обрабатываемой на СВТ, и предотвращению несанкционированного доступа к ней, в которой отражаются особенности использования оргтехники для обработки информации. Данная инструкция должна определять:

-систему доступа пользователей к информационным ресурсам и сведениям, составляющим конфиденциальную информацию;

-ответственность за разглашение конфиденциальной информации; - порядок разграничения допуска к работе на СВТ и регистрации пользователей;

-порядок изменения состава и конфигурации технических и программных средств;

-обязанности пользователей по подготовке и изданию конфиденциальных документов при работе на СВТ;

-обязанности должностных лиц по поддержанию работоспособности СВТ и средств защиты информации;

-порядок взаимодействия с информационными сетями общего пользования (Интернет) и пользования электронной почтой;

-порядок работы с базами данных, содержащими конфиденциальную информацию;

-порядок антивирусного обеспечения;

-организацию и технологию делопроизводства конфиденциальных документов;

-порядок контроля выполнения мероприятий по обеспечению защиты информации, обрабатываемой на СВТ.

При необходимости состав проводимых мероприятий по защите информации может быть дополнен в соответствии с решаемыми задачами и конкретными условиями применения средств вычислительной техники Администрации (муниципальных учреждений).

Основными направлениями защиты информации, обрабатываемой в АС либо на СВТ, являются:

-обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД и специальных воздействий;

-обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

Основные меры защиты информации в АС либо СВТ:

-реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;

-ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;

-разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

-использование источников бесперебойного питания для АС;

-регистрация действий пользователей АС обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

-учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;

-использование сертифицированных по требованиям безопасности информации специальных защитных знаков для контроля доступа к объектам защиты и для защиты документов от подделки;

-использование сертифицированных средств защиты информации; -размещение объектов защиты на максимально возможном расстоянии от границы контролируемой зоны;

-использование защищенных каналов связи;

-размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

-организация физической защиты помещений и технических средств обработки информации;

-предотвращение внедрения в АС программ-вирусов.

7.3. Распределенное хранение конфиденциальной информации, не разрешенной к открытому опубликованию, ее удаленная обработка и передача в локальных вычислительных сетях (далее – «ЛВС»), а также при межсетевом взаимодействии с другими ЛВС без выхода в сеть общего пользования типа Интернет, осуществляется только после установки на СВТ (АС) средств защиты информации от НСД и проведения аттестационных испытаний СВТ (АС) с целью официального подтверждения эффективности применяемых мер и средств защиты информации, отвечающих «Специальным требованиям и рекомендациям по технической защите конфиденциальной информации (СТР- К)», утвержденным приказом Гостехкомиссии (ФСТЭК) России от 30 августа 2002 года №282, и другим нормативным документам ФСТЭК России.

С целью обеспечения единой политики в организации работ по защите конфиденциальной информации, своевременного выявления предпосылок и предотвращения утечки информации по техническим каналам, НСД и непреднамеренных воздействий на информацию и средства ее обработки проводится периодический (не реже одного раза в год) контроль состояния защиты информации и оценка эффективности данных мероприятий.

Контроль состояния эффективности защиты информации осуществляется организацией - лицензиатом ФСТЭК России.

8. Ответственность за нарушение режима конфиденциальности

8.1. Должностные лица, принявшие решение об отнесении информации к категории ограниченного доступа, несут персональную ответственность за обоснованность принятого решения.

При приеме на работу каждый муниципальный служащий, либо работник Администрации, муниципального учреждения, предупреждается об ответственности за разглашение сведений конфиденциального характера, ставших ему известными в связи с выполнением им своих служебных обязанностей.

Допуск к конфиденциальной информации предусматривает оформленные в трудовом договоре обязательства и ответственность муниципального служащего, работника Администрации, муниципального учреждения, перед работодателем по нераспространению доверенной конфиденциальной информации.

Свои обязательства по сохранению сведений конфиденциального характера Администрации (муниципального учреждения) муниципальный служащий, либо работник Администрации, работник муниципального учреждения, подтверждает, подписывая обязательство о соблюдении требований обращения с защищаемой информацией (Приложение №2 к настоящему Положению).

Муниципальный служащий, либо работник Администрации, работник муниципального учреждения, несет персональную ответственность за разглашение сведений конфиденциального характера и обязан соблюдать правила обращения с конфиденциальной информацией и не разглашать ее, в том числе другим муниципальным служащим либо работникам Администрации, работникам муниципального учреждения, замещающим должность, не являющуюся должностью муниципальной службы, других структурных подразделений, за исключением случаев, когда это вызвано служебной необходимостью, соблюдая при этом установленные правила.

Каждый муниципальный служащий, либо работник Администрации, работник муниципального учреждения, обязан принимать меры по сохранности информации ограниченного распространения, предотвращению несанкционированной утечки (разглашения), искажения, блокирования или уничтожения используемой им в работе информации, подлежащей защите в соответствии с перечнем сведений конфиденциального характера.

Муниципальный служащий либо работник Администрации, работник муниципального учреждения не может использовать в личных целях сведения конфиденциального характера, ставшие ему известными вследствие выполнения служебных обязанностей.

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими информацию конфиденциального характера, муниципальный служащий либо работник администрации, работник муниципального учреждения, привлекается к дисциплинарной или иной предусмотренной законодательством ответственности.

Муниципальный служащий либо работник Администрации, работник муниципального учреждения, может быть привлечен к дисциплинарной,

административной (статья 13.14 «Кодекса Российской Федерации об административных правонарушениях», статья 243, п.7 «Трудового кодекса Российской Федерации»), уголовной (статьи 137,183, 272, 273 и 274 «Уголовного кодекса Российской Федерации») и гражданской (статья 857 «Гражданского кодекса Российской Федерации») ответственности, предусмотренной действующим законодательством Российской Федерации:

- за разглашение информации, доступ к которой ограничен (несанкционированную передачу третьим лицам);
- за нарушение режима защиты, обработки и порядка использования конфиденциальной информации;
- за неправомерный доступ к охраняемой компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно - телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации.

По фактам разглашения конфиденциальной информации руководителем назначается служебное расследование.

Если действиями (бездействием) работника, связанными с нарушением правил обращения с конфиденциальной информацией, причинен материальный ущерб Администрации (муниципальному учреждению), возмещение ущерба производится в порядке, предусмотренном законодательством Российской Федерации и трудовым договором.

Приложение №1
к Положению о порядке организации и
проведения работ по защите
конфиденциальной информации в
администрации МО «Токсовское городское
поселение» и подведомственных ей
муниципальных учреждениях

СВОДНЫЙ ПЕРЕЧЕНЬ
сведений конфиденциального характера

1. Данный сводный перечень сведений конфиденциального характера (далее – «Перечень») составлен на основании нормативных правовых актов Российской Федерации, относящих сведения к категории конфиденциальных. Перечень составляет правовую основу для проведения работ по защите информации и обеспечивает единый подход к отнесению сведений, используемых в деятельности органов исполнительной власти, государственных органов власти, органов местного самоуправления и подведомственных им учреждений к категории конфиденциальных, за исключением сведений, отнесенных к государственной тайне.

2. Конфиденциальность сведений, содержащихся в документах и обрабатываемых в средствах вычислительной техники, определяется по настоящему Перечню.

3. Конфиденциальность документов, составленных на основании материалов, поступивших из других организаций, определяется степенью конфиденциальности сведений, содержащихся в этих материалах.

№ п/п	Наименование сведений конфиденциального характера	Основания для включения в Перечень
	Сведения о гражданах	
1	Сведения о частной жизни лиц, за исключением сведений, подлежащих распространению в установленных федеральными законами случаях и предоставленных для опубликования в средствах массовой информации	ст. 24 «Конституции Российской Федерации»
2	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях	п. 1 Указа Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»
3	Сведения о частной жизни лица, составляющие его личную или семейную тайну	ст. 137 «Уголовного кодекса Российской Федерации»

4	Информация о гражданах (персональные данные: сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность	ст. 3, Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных»
5	Информация о работниках (персональные данные), необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника	ст. 85, 86 «Трудового кодекса Российской Федерации»
6	Сведения об абонентах и оказываемых им услугах связи, сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, переводимые денежные средства, телеграфные и иные сообщения	ст. 53, 63 Федерального закона от 7 июля 2003 года №126-ФЗ «О связи»
7	Информация об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения	ст. 15 Федерального закона от 17 июля 1999 года №176- ФЗ «О почтовой связи»
8	Сведения, ставшие известными работникам органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния.	ст. 12 Федерального закона от 15 ноября 1997 года №143-ФЗ «Об актах гражданского состояния»
9	Сведения личного характера, ставшие известными работнику учреждений социального обслуживания при оказании социальных услуг	ст. 4, 6 Федерального закона от 28 декабря 2013 года №442- ФЗ «Об основах социального обслуживания граждан в Российской Федерации»
10	Сведения о доходах, об имуществе и обязательствах имущественного характера муниципальных служащих	ст. 20 Федерального закона от 27 июля 2004 года №79- ФЗ «О государственной гражданской службе Российской Федерации»
11	Сведения о населении, содержащиеся в переписных листах.	ст. 8 Федерального закона от 25 января 2002 года №8-ФЗ «О Всероссийской переписи населения»

12	Сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц	ст. 17 Федерального закона от 1 апреля 1996 года № 27- ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»
13	Сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц	ст. 946 «Гражданского кодекса Российской Федерации»
14	Любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.	ст. 8 Федерального закона от 31 мая 2002 года №63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»
15	Обстоятельства, которые стали известны священнослужителю из исповеди.	ст. 3 Федерального закона от 26 сентября 1997 года№ 125- ФЗ «О свободе совести и о религиозных объединениях»
16	Сведения о результатах обследования лица, вступающего в брак	ст. 15 «Семейного кодекса Российской Федерации»
17	Информационные ресурсы, циркулирующие в ГАС «Выборы», а именно персональные данные, независимо от уровня и способа их формирования.	ст. 17 Федерального закона от 10 января 2003 года № 20- ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы»»
18	Сведения о детях, оставшихся без попечения родителей, и гражданах, желающих принять детей на воспитание в свои семьи попечения родителей»	ст. 8 Федерального закона от 16 апреля 2001 года № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей»

Сведения о профессиональной деятельности		
19	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральным законодательством (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений и т. д.)	п. 4 Указа Президента Российской Федерации от 06 марта 1997 гола№ 188 «Об утверждении перечня сведений конфиденциального характера»
20	Сведения о наличии у гражданина психического расстройства, фактах обращения за психиатрической помощью и лечения в учреждении, оказывающем такую помощь, а также иные сведения о состоянии психического здоровья	ст. 9 Закона Российской Федерации от 2 июля 1992 года№ 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»
21	Сведения, которые стали известны нотариусу в связи с совершением нотариальных действий, в там числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных в «Основах законодательства о нотариате»	ст. 5 «Основы законодательства РФ о нотариате» от 11 февраля 1993 года № 4462-1
22	Материалы, полученные при рассмотрении жалоб, до вынесения окончательного решения по ним, сведения о частной жизни заявителя и других лиц без их письменного согласия	ст. 28 Федерального Конституционного закона от 26 февраля 1997 года №1- ФКЗ «Об Уполномоченном по правам человека в Российской Федерации»
23	Информация, содержащаяся в медицинских документах гражданина. Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении	ст. 4, 13 Федерального закона от 21 ноября 2011 года №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
24	Сведения о доноре и реципиенте при трансплантации органов	ст. 14 Закона Российской Федерации от 22 декабря 1992 года №4180-1 «О трансплантации органов и (или) тканей человека»
25	Сведения о проведенных искусственных оплодотворении и имплантации эмбриона, а также о личности донора	ст. 4, 13 Федерального закона от 21 ноября 2011 года №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
26	Информация о новых решениях и технических знаниях, в том числе не защищаемых законом, полученных благодаря исполнению своих обязательств по договору подряда, а также сведения, которые могут рассматриваться как коммерческая тайна	ст. 727 «Гражданского кодекса Российской Федерации»

27	Первичная геологическая, геофизическая, геохимическая и иная информация, данные по ее интерпретации и производные данные, полученные в результате выполнения работ по соглашению о разделе продукции	ст. 11 Федерального закона от 30 декабря 1995 года № 225-ФЗ «О соглашениях о разделе продукции»
28	В распространяемых средствами массовой информации: - сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне, за исключением случаев, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом; - сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя; - сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, признанного потерпевшим, без согласия самого несовершеннолетнего и (или) его законного представителя	ст. 41 Закона Российской Федерации от 27 декабря 1991 года №2124-1 «О средствах массовой информации»
29	Сведения, содержащиеся в регистрах бухгалтерского учета, внутренней бухгалтерской отчетности организаций	ст. 10 Федерального закона от 6 декабря 2011 года №402- ФЗ «О бухгалтерском учете»
30	Сведения о мерах безопасности (перевод на другую работу, временное помещение в безопасное место, переселение на другое место жительства, замена документов и т.д.), применяемых в отношении должностного лица правоохранительного или контролирующего органа	ст. 320 «Уголовного кодекса Российской Федерации»
31	Информация, полученная в ходе проверки финансово- хозяйственной деятельности лиц, осуществляющих внешнеэкономические операции с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности	ст. 15,17 Федерального закона от 18 июля 1999 года № 183-ФЗ «Об экспортном контроле»

32	Сведения, касающиеся предмета договора на выполнение научно-исследовательских работ, опытно- конструкторских и технологических работ, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре	ст. 771 «Гражданского кодекса Российской Федерации»
33	Сведения об операциях, счетах и вкладах клиентов и корреспондентов, а также иные сведения, устанавливаемые кредитной организацией, если это не противоречит федеральному закону	ст. 26 Федерального закона от 2 декабря 1990 года №395- 1 «О банках и банковской деятельности»
34	Сведения о налогоплательщике с момента постановки на учет, если иное не предусмотрено Налоговым кодексом Российской Федерации	ст. 84, 102 части первой «Налогового кодекса Российской Федерации»
35	Содержание данных налогового учета (в том числе данных первичных документов)	ст. 313 части второй «Налогового кодекса Российской Федерации»
36	Сведения, содержащиеся в документах, получаемых и составляемых аудитором в ходе аудиторской проверки, если на разглашение их содержания нет согласия собственника (руководителя) Федерации, экономического субъекта, за исключением случаев, предусмотренных законодательными актами Российской Федерации	ст. 8 Федерального закона от 30 декабря 2008 года № 307- ФЗ «Об аудиторской проверке деятельности»
37	Сведения, раскрывающие данные предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения.	ст. 310 «Уголовного кодекса Российской Федерации»

38	Суждения, имевшие место во время совещания присяжных заседателей в совещательной комнате (тайна совещания присяжных заседателей)	ст. 341 «Уголовно-процессуального кодекса Российской Федерации»
39	Суждения, имевшие место при обсуждении и постановлении приговора в совещательной комнате	ст. 298 «Уголовно-процессуального кодекса Российской Федерации»
40	Сведения о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких	ст. 311 «Уголовного кодекса Российской Федерации»
Сведения о коммерческой деятельности		
41	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с «Гражданским кодексом Российской Федерации» и федеральными законами	п. 5 Указа Президента Российской Федерации от 6 марта 1997 года №188 «Об утверждении перечня сведений конфиденциального характера»
42	Научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны)	ст. 3 Федерального закона от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»
43	Сведения, полученные пользователем по договору коммерческой концессии, раскрывающие секреты производства правообладателя	ст. 1032 «Гражданского кодекса Российской Федерации»
44	Сведения о банковском счете и банковском вкладе, операциях по счету и сведения о клиенте	ст. 857 «Гражданского кодекса Российской Федерации»
45	Информация, содержащаяся в заключении по результатам аудиторской проверки сельскохозяйственного кооператива, за исключением случаев, предусмотренных законом	ст. 33 Федерального закона от 8 декабря 1995 года №193- ФЗ «О сельскохозяйственной кооперации»
46	Геологическая и иная информация о недрах, полученная пользователем недр за счет собственных средств	ст. 27 Закона Российской Федерации от 21 февраля 1992 года №2395-1 «О недрах»

47	Конфиденциальные сведения о музейных предметах, включенных в состав негосударственной части Музейного фонда Российской Федерации	ст. 38 Федерального закона от 26 мая 1996 года №54-ФЗ «О Музейном фонде Российской Федерации и музеях в Российской Федерации»
Сведения служебного характера		
48	К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью	п. 1.2. Положения о порядке обращения со служебной информацией ограниченного распространения в органах исполнительной власти, утвержденного постановлением Правительства Российской Федерации от 3 ноября 1994 года №1233
49	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с «Гражданским кодексом Российской Федерации» и федеральными законами (коммерческая тайна)	п. 3 Указа Президента Российской Федерации от 6 марта 1997 гола №188 «Об утверждении перечня сведений конфиденциального характера»
50	Информация, полученная в процессе сбора, хранения, передачи и использования сведений, содержащихся в пенсионных счетах негосударственного пенсионного обеспечения, пенсионных счетах накопительной части трудовой пенсии, а также при выплате негосударственной пенсии н накопительной частя трудовой пенсии, выплатах (переводе) выкупных сумм и выплатах правопреемникам	ст. 15 Федерального закона от 7 мая 1998 года № 75-ФЗ «О негосударственных пенсионных фондах»
51	Сведения о специальных средствах, технических приемах, тактике осуществления мероприятий по борьбе с терроризмом, в также о составе их участников	ст. 2 Федерального закона от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму»
52	Государственная статистическая отчетность по конкретному хозяйствующему субъекту.	Перечень служебной информации ограниченного распространения, утвержденный председателем Госкомстата Россия 14 февраля 2002 года

53	Информация, составляющая служебные сведения (ДСП), связанные с исполнением функций при выполнении работ по видам деятельности в соответствии с действующим законодательством Российской Федерации	Указ Президента РФ от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»

Приложение № 2
к Положению о порядке организации и
проведения работ по защите
конфиденциальной информации в
администрации МО «Токсовское городское
поселение» и подведомственных ей
муниципальных учреждениях

Обязательство о соблюдении требований обращения с защищаемой информацией

_____

Наименование органа

в лице руководителя _____

(Ф.И.О)

с одной стороны, и _____

(Ф.И.О., должность)

с другой стороны, заключили настоящее соглашение о том, что

_____

(Ф.И.О., должность)

будет предоставлен доступ к конфиденциальным и другим защищаемым сведениям, необходимым ему для выполнения своих функциональных обязанностей (согласно занимаемой должности). _____

Обязуется:

1. Принимать меры по сохранности сведений конфиденциального характера, ставших ему известными в связи с выполнением им своих служебных обязанностей (хранить служебную тайну).

2. Во время работы в _____

(орган местного самоуправления, учреждение) _____

и в течение 3-х лет после увольнения не раскрывать (не передавать) третьим лицам, в том числе другим сотрудникам структурных подразделений, ставшие ему известными конфиденциальные сведения, за исключением случаев, когда это вызвано служебной необходимостью, соблюдая при этом установленные требования и правила.

3. Не использовать ставшие ему известными или разработанные им конфиденциальные сведения иначе, как в интересах

_____

(орган местного самоуправления, учреждение)

4. Соблюдать указанные в Положении по защите конфиденциальной информации требования и правила обеспечения информационной безопасности

_____

(орган местного самоуправления, учреждение)

5. В случае прекращения работы в

_____
(орган местного самоуправления, учреждение)

сразу же сдать все документы и другие материалы, содержание которых отнесено к конфиденциальной и иной защищаемой информации.

Работник администрации либо работник муниципального учреждения может быть привлечен к дисциплинарной, административной (статья 13.14 «Кодекса Российской Федерации об административных правонарушениях», статья 243, п.7 «Трудового кодекса Российской Федерации», уголовной (статьи 137,183, 272, 273 и 274 «Уголовного кодекса Российской Федерации») и гражданской (статья 857 «Гражданского кодекса Российской Федерации») ответственности, предусмотренной действующим законодательством Российской Федерации:

- за разглашение информации, доступ к которой ограничен несанкционированную передачу третьим лицам);
- за нарушение режима защиты, обработки и порядка использования конфиденциальной информации;
- за неправомерный доступ к охраняемой компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Работник администрации, либо работник муниципального учреждения может быть привлечен к возмещению ущерба в соответствии с порядком, предусмотренным действующим законодательством Российской Федерации, если его действиями (бездействием), связанными с нарушением правил обращения с конфиденциальной информацией, причинен материальный ущерб.

Работник администрации, либо работник муниципального учреждения подтверждает, что:

- он (она) ознакомлен(а) с требованиями Положения о порядке организации и проведения работ по защите конфиденциальной информации в администрации МО «Токсовское городское поселение» и подведомственных ей муниципальных учреждениях;
- он (она) не имеет перед кем-либо никаких обязательств, которые входят в противоречие с настоящим обязательством или ограничивают его (ее) деятельность в

_____
(орган местного самоуправления, учреждение)

"___" _____ 20__ г.

_____ _____
(подпись) (Ф.И.О. работника)