**АДМИНИСТРАЦИЯ**

**ВАРЛАМОВСКОГО СЕЛЬСОВЕТА БОЛОТНИНСКОГО РАЙОНА**

**НОВОСИБИРСКОЙ ОБЛАСТИ**

**ПОСТАНОВЛЕНИЕ № 53**

**от 23.05.2012 г. с.Варламово**

**Об утверждении должностной инструкции ответственного за организацию защиты персональных данных в администрации Варламовского сельсовета**

В соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных», Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г., Постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Положением по обработке и защите персональных данных в администрации Варламовского сельсовета, утверждённого Постановлением администрации Варламовского сельсовета от 23.05.2012 № 51 «Об утверждении Положения по обработке и защите персональных данных в администрации Варламовского сельсовета»,

**ПОСТАНОВЛЯЮ:**

1. Утвердить должностную инструкциюответственного за организацию защиты персональных данных в администрации Варламовского сельсовета, согласно приложения.
2. Опубликовать настоящее постановление в официальном вестнике Варламовского сельсовета и разместить на официальном сайте администрации Варламовского сельсовета.
3. Настоящее постановление вступает в законную силу после дня его подписания.
4. Контроль за исполнением настоящего Постановления оставляю за собой.

Глава Варламовского сельсовета: /А.В.Приболовец/

Приложение к постановлению администрации Варламовского сельсовета Болотнинского района Новосибирской области от 23.05.2012 г. № 53

**Должностная инструкция**

**ответственного за организацию защиты персональных данных в администрации Варламовского сельсовета**

**1. Общие положения**

1. Настоящая должностная Инструкция (далее – Инструкция) разработана для обеспечения защиты персональных данных в администрации Варламовского сельсовета. Персональные данные (ПДн) относятся к категории информации ограниченного распространения.

2. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;

- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;

- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

3. Работа с персональными данными строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;

- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

**2. Обязанности работников, имеющих доступ к ПДн**

4. Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать руководителя структурного подразделения, специалиста по защите информации.

5. Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

6. В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Правительства области, полученные в течение срока работы.

3. ***Работники при работе с персональными данными обязаны:***

3.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

3.2. Выполнять требования администратора безопасности, касающиеся защиты информации;

3.3. Знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

3.4. Хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;

3.5. Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);

3.6. Контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы.

3.7. Немедленно ставить в известность руководителя администрации Варламовского сельсовета:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;

- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.

3.8. В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

3.9. Ставить в известность администратора безопасности администрации Варламовского сельсовета при:

- необходимости обновления антивирусных баз;

- обновлении программного обеспечения;

- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;

- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;

- резервном копировании информации;

- и т.д.

3.10. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

3.11. Вынос ПЭВМ, на которой проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

3.12. ПЭВМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

**4. Запрещается:**

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;

- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;

- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;

- накапливать ненужные для работы персональные данные;

- передавать или принимать без расписки документы ограниченного распространения;

- оставлять на рабочих столах, в столах и незакрытых сейфах документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера.

- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;

— самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

— осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

— записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);

— оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

— умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения, ответственного за техническое и (или) программное обеспечение, администратора безопасности.

**5. Права специалиста**

Специалист имеет право:

5.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

5.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

5.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

5.4. Контролировать деятельность структурных подразделений соответствующей организации в части выполнения ими требований по обеспечению безопасности персональных данных.

5.5. Вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

**6. Ответственность**

6.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

6.2. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

**С инструкцией ознакомлены:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность, Ф.И.О. , подпись, расшифровка подписи)