**ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ АКТАНЫШСКОГО МУНИЦИПАЛЬНОГО РАЙОНА РЕСПУБЛИКИ ТАТАРСТАН**

пр. Ленина, дом 17, с.Актаныш, 423740

**ТАТАРСТАН РЕСПУБЛИКАСЫ АКТАНЫШ МУНИЦИПАЛЬ РАЙОНЫ БАШКАРМА КОМИТЕТЫ**

Ленин пр.,17 йорт, Актаныш ав., 423740

Тел. (85552) 3-02-22, факс (85552) 3-13-44, E-mail: mail.Aktanish@tatar.ru , www.aktanysh.tatarstan.ru

КАРАР
от 06.09.2018

ПОСТАНОВЛЕНИЕ
№ ПР-221

**Об информационной безопасности и защите персональных данных в Исполнительном комитете Актанышского муниципального района**

В связи с актуализацией вопросов информационной безопасности и защиты персональных данных постановляю:

1. Утвердить положение о постоянно действующей технической комиссии (приложение 1).
2. Утвердить состав постоянно действующей технической комиссии (приложение 2).
3. Утвердить политику информационной безопасности (приложение 3).
4. Утвердить положение об обработке персональных данных (приложение 4).
5. Утвердить перечень сведений конфиденциального характера (приложение 5).
6. Утвердить положение о специалисте по информационной безопасности (приложение 6).
7. Утвердить положение о категорировании информационных ресурсов (приложение 7).
8. Утвердить регламент доступа в помещения с серверным и телекоммуникационным оборудованием (приложение 8).
9. Утвердить положение о порядке обращения с информацией конфиденциального характера (приложение 9).

И. о. Руководителя
Исполнительного комитета Л. Р. Сираева

Приложение № 1
К постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2018 № ПР-221

**Положение**
**о постоянно действующей технической комиссии**
**по защите персональных данных**

## 1. Общие положения

1.1. Постоянно действующая техническая комиссия по защите персональных данных (далее – ПДТК) при Исполнительном комитете Актанышского муниципального района создана в целях выработки предложений и рекомендаций по вопросам, связанным с защитой персональных данных:

1.1.1. Своевременное выявление и закрытие возможных каналов неправомерного распространения сведений, являющихся персональными данными (далее – ПД).

1.1.2. Организация и координация работ по противодействию иностранным техническим разведкам (далее – ПД ИТР) и технической защите информации.

1.1.3. Совершенствование системы физической и технической защиты здания Исполнительного комитета Актанышского муниципального района, направленной на обеспечение его безопасности.

1.1.4. Проведение в случаях и порядке, установленных законодательством, экспертизы материалов, предназначенных для открытого опубликования и вывоза за границу.

1.2. ПДТК является коллегиальным совещательным органом при Исполнительном комитете Актанышского муниципального района Актанышского района и осуществляет свою деятельность на общественных началах.

1.3. ПДТК подотчетна и подконтрольна непосредственно Руководителю Исполнительного комитета Актанышского муниципального района.

1.4. Состав ПДТК утверждается постановлением Руководителя Исполнительного комитета Актанышского муниципального района.

1.5. ПДТК в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации,

законами и нормативными правовыми актами Республики Татарстан, нормативно-правовыми актами муниципального образования «Актанышский муниципальный район» и настоящим Положением.

## 2. Основные функции ПДТК

Основными функциями ПДТК являются:

2.1. Организация, методическое обеспечение и проведение аналитической работы по предупреждению утечки и комплексной защите сведений, являющихся ПД.

2.2. Разработка нормативной правовой, научно-технической и методической баз по вопросам выявления и закрытия возможных каналов неправомерного распространения сведений, являющихся ПД, в том числе по ПД ИТР, защите информационных систем, а также по совершенствованию системы физической защиты здания Исполнительного комитета Актанышского муниципального района.

2.3. Разработка комплекса мер по защите ПД при осуществлении научно-технического и экономического сотрудничества с зарубежными странами, в том числе при выезде за границу лиц, осведомленных в сведениях, являющихся ПД, и при посещении отделов в здании Исполнительного комитета Актанышского муниципального района лицами не являющимися сотрудниками отделов Исполнительного комитета Актанышского муниципального района.

2.4. Разработка комплекса мер по обеспечению охраны здания Исполнительного комитета Актанышского муниципального района, организации внутри объектового и пропускного режима.

2.5. Изучение и анализ возможностей иностранных технических разведок с учетом профиля работ и оперативной обстановки в Исполнительном комитете Актанышского муниципального района, определение видов и средств разведки, которым необходимо оказывать противодействие.

2.6. Разработка системы мер ПД ИТР, защиты информационных систем и сведений, являющихся ПД.

2.7. Организация и координация разработки, внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами.

2.8. Организация и проведение работ по контролю за эффективностью принимаемых мер по выявлению и закрытию возможных каналов неправомерного распространения сведений, являющихся ПД, а также по совершенствованию системы физической защиты здания Исполнительного комитета Актанышского муниципального района.

2.9. Подготовка заключений о возможности эксплуатации помещений, в которых осуществляются обработка и хранение документированной информации, содержащей сведения, составляющие государственную тайну, и проведение работ, связанных обработкой ПД.
2.10. Проведение анализа обстоятельств и причин неправомерного распространения сведений, являющихся ПД.
2.11. Подготовка предложений по совершенствованию действующей в Исполнительном комитете Актанышского муниципального района системы защиты сведений, являющихся ПД.

## 3. Полномочия ПДТК

Для осуществления своей деятельности ПДТК вправе:
3.1. Запрашивать и получать в установленном порядке от структурных подразделений Исполнительного комитета Актанышского муниципального района материалы и сведения, необходимые для выполнения задач, возложенных на ПДТК.
3.2. Проводить заседания ПДТК, принимать решения и вести переписку по всем вопросам, входящим в компетенцию ПДТК.
3.3. Привлекать в установленном порядке к работе ПДТК специалистов для проведения экспертиз и составления заключений по вопросам, отнесенным к компетенции ПДТК.
3.4. Вносить на рассмотрение Руководителю Исполнительного комитета, предложения по вопросам, отнесенным к компетенции ПДТК.
3.5. Создавать рабочие группы (далее – группы) внутри ПДТК по отдельным вопросам, возникающим в процессе работы, и направлениям ее деятельности. Персональный состав, задачи и порядок работы групп утверждаются ПДТК.

## 4. Организация и обеспечение деятельности ПДТК

4.1. ПДТК осуществляет свою деятельность в соответствии с разработанным планом, который утверждается Руководителем Исполнительного комитета Актанышского муниципального района.

Материалы к обсуждению на заседаниях ПДТК готовятся ее членами или по поручению председателя ПДТК специалистами соответствующих отделов.
4.2. Заседания ПДТК проводятся по мере необходимости, но не реже одного раза в квартал. При необходимости на заседания ПДТК могут приглашаться компетентные в рассматриваемых вопросах сотрудники исполнительных органов государственной власти Актанышского района, а также представители федеральных органов защиты государственной тайны и других

заинтересованных организаций, имеющие допуск к обработке персональных данных по соответствующей форме.

4.3. ПДТК возглавляет председатель, который организует работу ПДТК и имеет следующие полномочия:

4.3.1. Координирует деятельность членов ПДТК по выполнению возложенных на ПДТК задач.

4.3.2. Созывает очередные и внеочередные заседания ПДТК, формирует повестку дня с учетом требований руководящих документов по защите ПД и предложений членов ПДТК.

4.3.3. Ведет заседания ПДТК.

4.3.4. Утверждает повестку дня, дату, время и место проведения очередного заседания ПДТК.

4.3.5. Выполняет иные функции по обеспечению деятельности ПДТК.

4.4. В случае отсутствия председателя ПДТК его функции выполняет его заместитель.

4.5. Выполнение технической работы ПДТК организует секретарь ПДТК, который отвечает за подготовку заседаний, оформляет протоколы ее заседаний, контролирует выполнение решений ПДТК и готовит отчеты о ее работе.

4.6. Решения ПДТК принимаются простым большинством голосов от присутствующих на заседании членов ПДТК и оформляются протоколом.

4.7. Протоколы заседания ПДТК подписываются председателем и секретарем, а в отсутствие председателя – его заместителем.

## 5. Контроль за работой ПДТК

5.1. ПДТК подотчетна Руководителю Исполнительного комитета Актанышского муниципального района. Председатель ПДТК периодически, но не реже одного раза в год, отчитывается перед Руководителем Исполнительного комитета Актанышского муниципального района об итогах работы ПДТК и реализации ее предложений и рекомендаций.

Приложение №2
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2016 № 777-2016

**Состав**
**постоянно действующей технической комиссии по защите персональных данных**

| Председатель | Должность |
|---|---|
| Тимиров Альберт Индарифович | заместитель Руководителя Исполнительного комитета Актанышского муниципального района |
| Члены комиссии: | |
| Харисова Гульназ Илгизовна | начальник отдела информатизации Исполнительного комитета Актанышского муниципального района |
| Имамова Галина Ибрахимовна | начальник отдела бухгалтерского учета и отчетности аппарата Совета Актанышского муниципального района |
| Аглетдинова Алия Мансуровна | заместитель начальника организационного отдела (по кадрам) аппарата Совета Актанышского муниципального района |

Приложение №3
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 16.09.2021 № 890-21

**Политика информационной безопасности**
**Актанышского муниципального района**

## 1. Общие положения

Политика информационной безопасности Актанышского муниципального района предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах района, управления и контроля информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

В структуру Актанышского муниципального района (далее – район) входят: Совет и Исполнительный комитет муниципального района, структурные подразделения Исполнительного комитета, а также все сельские поселения района.

Политика информационной безопасности отражает позицию руководства района по вопросу обеспечения информационной безопасности района.

Политика информационной безопасности района направлена на:

нормативное регулирование процесса обмена защищаемой информацией района с взаимодействующими структурами, юридическими и физическими лицами;

установление определенного организационно-правового режима использования информационных ресурсов района;

разработку системы нормативных документов района, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации района, ответственность должностных лиц и сотрудников за соблюдение этих требований;

реализацию комплекса организационных, инженерно-технических, технических и аппаратно-программных мероприятий по предупреждению несанкционированных действий с информацией и защиту ее от утечки по техническим каналам;

предоставление пользователям необходимых сведений для сознательного поддержания установленного уровня защищенности объектов информатизации района;

организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения информационной безопасности района;

создание в районе резервов и возможностей по ликвидации последствий нарушения режима защиты информации и восстановления системы обеспечения информационной безопасности.

Настоящий документ разработан в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005.

## 2. Цель обеспечения информационной безопасности

Основной целью является обеспечение информационной безопасности района, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

Главная цель принимаемых мер защиты информации района состоит в том, чтобы гарантировать целостность, достоверность, доступность и конфиденциальность информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах (далее - информационные системы) района, независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности района, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности района несет Руководитель Исполнительного комитета. Отдел информатизации и защиты информации осуществляет разработку проектов объектов информатизации в защищенном исполнении и их эксплуатацию с учетом требований по защите информации. Методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет начальник отдела информатизации и защиты информации.

## 3. Объекты информационной безопасности района

Объектом защиты в контексте данной Политики являются информационные ресурсы района, обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем района.

Основными объектами защиты района являются:

информационные ресурсы района, содержащие сведения, отнесенные к государственной тайне;

информационные ресурсы района, ограниченного распространения, в том числе, содержащие конфиденциальные сведения;

информационные ресурсы района, представляющие коммерческую ценность;

программные информационные ресурсы района, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

физические информационные ресурсы района: компьютерное аппаратное обеспечение всех видов; носители информации всех видов (электронные, бумажные и проч.);

все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;

технические сервисы района (отопление, освещение, энергоснабжение, кондиционирование воздуха и т.п.).

Следует также отметить, что указанные выше основные объекты защиты являются наиболее ценными ресурсами, и, следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа района, эффективности его функционирования и т.д. Доступность, целостность и конфиденциальность в обязательном порядке должны учитываться при разработке организационно-распорядительной документации по обеспечению информационной безопасности для системы в целом и для каждого ее ресурса в отдельности.

## 4. Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности района являются:

инвентаризация и систематизация всех информационных ресурсов района;

обеспечение безопасности информационных ресурсов района: уменьшение риска их случайной или намеренной порчи, уничтожения или хищения;

сведение к минимуму финансовых, временных и прочих потерь, связанных с нарушением информационной безопасности и физическими неисправностями аппаратного и программного обеспечения, а также осуществление мониторинга и реагирование по случаям инцидентов;

обеспечение безопасной, четкой и эффективной работы сотрудников района с его информационными ресурсами;

сведение к разумному минимуму финансовых затрат на поддержание функционирования аппаратного и программного обеспечения и автоматизированной системы в целом на должном уровне (сюда относятся крупные и мелкие обновления программного и аппаратного обеспечения, бесперебойное обеспечение системы расходными материалами и проч.);

сведение пользования информационными ресурсами к единой системе организационно-распорядительной документации.

## 5. Принципы обеспечения информационной безопасности района

При построении системы защиты необходимо придерживаться следующих принципов:

применение разнородных систем обеспечения информационной безопасности;

достоинства одних частей системы обеспечения информационной безопасности должны перекрывать недостатки других;

система обеспечения информационной безопасности должна строиться многоуровневой;

в зоне максимальной безопасности должны располагаться особо важные информационные ресурсы;

непрерывность и целенаправленность процесса обеспечения информационной безопасности;

усиление защиты информации во время нештатных ситуаций;

обеспечение возможности регулирования уровня информационной безопасности без изменения функциональной базы системы информационной безопасности;

обеспечение простоты в применении механизмов защиты для рядовых сотрудников района.

## 6. Оценка рисков

Для оценки рисков при составлении и последующем пересмотре организационно-распорядительных документов необходимо систематически рассматривать следующие аспекты:

ущерб, который может нанести деятельности района серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

реальную вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

## 7. Требования в отношении обучения вопросам информационной безопасности

Основной целью обучения является:

обеспечение уверенности в осведомленности сотрудников района об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством;

знание сотрудниками правильного использования средств обработки информации прежде чем им будет предоставлен доступ к информации или услугам;

оснащение сотрудников района всем необходимым для соблюдения требований политики безопасности района при выполнении служебных обязанностей.

Сотрудники района должны знать и выполнять требования организационно-распорядительных документов (в части касающейся) района в области информационной безопасности, требования обеспечения безопасности обработки информации на средствах вычислительной техники, правила работы в сети Интернет.

Сотрудники района должны уметь работать с системой электронного документооборота; операционными системами MS Wndows на уровне пользователя, антивирусным программным обеспечением, офисным программным обеспечением (MS Word, MS Excel. MS Power Point), должны уметь пользоваться встроенной справкой.

Специалисты отдела информатизации и защиты информации совместно с начальником отдела должны обучать сотрудников района правильному использованию средств обработки защиты информации, чтобы свести к минимуму возможные риски безопасности.

Все сотрудники района и, при необходимости, пользователи третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик информационной безопасности, принятых в районе.

## 8. Правила физической защиты

Перед внедрением и использованием нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо разработать для него правила обеспечения безопасности и использовать их наряду с правилами, изложенными в данном разделе.

Перед установкой и использованием какого-либо компьютерного аппаратного обеспечения в обязательном порядке следует ознакомиться с информацией, предоставленной разработчиком (продавцом), и строго ей следовать.

Перед проведением крупной модернизации или ремонта, перед выполнением манипуляций непосредственно с носителями информации необходимо выполнить резервное копирование данных.

После выполнения процесса модернизации аппаратного и/или программного обеспечения необходимо обязательно провести внеплановое техническое обслуживание всей системы.

При размещении компьютерного оборудования в помещении, а также в процессе его эксплуатации приоритетным является обеспечение для него безопасного функционирования, соответствующего положениям, изложенным в прилагаемой к нему документации. В период простоя устройства необходимо обеспечить сохранность его работоспособности и внешнего вида.

Все приобретенное компьютерное аппаратное и программное обеспечение должно регистрироваться в специальном журнале с указанием подробной информации о его покупке. Также следует тщательно регистрировать все действия по модернизации компьютерного аппаратного и программного обеспечения.

Всю документацию на компьютерное оборудование и программное обеспечение (гарантийные обязательства производителей/продавцов, руководства пользователей (User's Manual), регистрационные карточки, кассовые и товарные чеки и проч.) должны обязательно сохраняться после покупки и храниться в надежном, защищенном от света и других вредоносных воздействий месте в упаковке.

Следует в полном объеме и неукоснительно соблюдать правила эксплуатации тех или иных аппаратных компьютерных компонентов.

Техническое обслуживание компьютерного оборудования и программного обеспечения (физическая чистка оборудования, поддержание программного обеспечения в работоспособном состоянии и т.д.) следует производить регулярно, желательно в соответствии с заранее составленным расписанием и с учетом рекомендаций разработчиков данного оборудования и программ (с данными рекомендациями следует внимательно ознакомиться до выполнения каких-либо действий по обслуживанию).

Техническим обслуживанием считаются также и мероприятия по резервному копированию данных, которые должны неукоснительно исполняться. Они должны выполняться строго регулярно и не реже, чем раз в неделю. Если это возможно, стоит сделать повторную копию данных и разместить ее на хранение отдельно от первой. Сразу же после проведения резервного копирования данных необходимо каким-либо способом убедиться в работоспособности и корректности полученной копии.

Резервному копированию в обязательном порядке подлежат:

все конфиденциальные данные сотрудников в автоматизированной системе;

все исходные материалы для разработки собственного программного обеспечения и прочих проектов;

такие данные системы, без которых невозможна ее нормальная работа;

все прочие важные данные, которые записаны на физически ненадежных носителях информации и носителях, поддерживающих операции перезаписи;

любые другие данные согласно решению уполномоченных сотрудников района.

Во время резервного копирования данных, а также во время записи любой информации на носители информации однократной записи, нельзя производить другие виды работ на той компьютерной системе, при помощи которой осуществляется эта запись.

Все носители (электронные, бумажные и все другие) с конфиденциальной информацией и резервными копиями этой и другой информации сотрудника района должны храниться в недоступном для посторонних, защищенном от света и других вредоносных воздействий месте с соблюдением правил безопасного хранения для данного вида носителя информации. Носителям с особо ценной информацией следует уделять повышенное внимание.

Все расходные материалы следует использовать максимально эффективно, не допуская нерационального их использования. Все расходные материалы

(используемые в данный момент и неиспользуемые) необходимо хранить в строгом соответствии с правилами их хранения.

Желательно предпринять ряд мер по энергосбережению для тех устройств, которые временно не используются или находятся в состоянии ожидания.

Запрещается курить, употреблять пищу и напитки непосредственно вблизи компьютера. Необходимо предпринять меры, чтобы обезопасить компьютерное оборудование от повреждения в данном случае.

В течение внедрения и использования нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо приложить все усилия к тому, чтобы научиться эффективно его применять.

Необходимо в обязательном порядке записать все наиболее важные установки и настройки системы в состоянии ее нормального (штатного) функционирования. Подобные записи приравниваются к аппаратно/программной документации, и должны соответствующим образом обслуживаться.

Необходимо размещать системы вывода информации (мониторы, дисплеи и т.д.) компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются.

Необходимо предпринять ряд мер, благодаря которым компьютерные системы пользователя будут обеспечены стабильным электропитанием. Обязательным является использование хотя бы самых простых средств по обеспечению надежности электропитания системы (сетевые фильтры, заземление и т.д.).

При возникновении какой-либо аварийной ситуации необходимо немедленно прекратить эксплуатацию аварийного устройства. Немедленно поставить в известность начальника отдела информатизации и защиты информации. Отделу информатизации и защиты информации в кратчайшие сроки организовать мероприятия по его ремонту или замене.

Следует составить подробные технологические схемы для проведения различного рода мероприятий, связанных с аппаратным и программным обеспечением (техническое обслуживание, правила техники безопасности, резервное копирование данных и т.п.).

Необходимо рассмотреть возможность применения различных систем автоматизированного мониторинга текущего состояния аппаратных информационных ресурсов, и при первой же возможности внедрить их, по крайней мере, на наиболее важных и ответственных участках.

В течение процесса списания компьютерной техники, носителей информации и др. необходимо позаботиться о том, чтобы после выполнения процедуры переноса основных информационных ресурсов со списываемой техники, было произведено полное и безвозвратное уничтожение содержащейся на ней конфиденциальной и любой другой информации.

Необходимо обязательно разработать план действий по продолжению работы и обеспечению безопасности данных на случай, если выйдут из строя какие-либо аппаратные и/или программные части компьютерной системы.

Данный план должен систематически проверяться на актуальность и при необходимости пересматриваться.

## 9. Правила внешнего доступа

После установки системы и перед первым выходом в сеть необходимо в обязательном порядке принять комплекс мер по установлению защиты от вредоносного воздействия сети.

В системе должны быть предприняты все возможные меры для предотвращения распространения в ней компьютерных вирусов, «червей» и прочей потенциально опасной для ее безопасности информации. Все сотрудники района обязаны принимать участие в реализации этих мер и никакими своими действиями не должны препятствовать их проведению.

Необходимо строго контролировать с помощью соответствующего программного обеспечения (антивирус, брандмауэр и проч.) всю входящую и исходящую информацию на наличие вирусов и прочей потенциально опасной информации. Необходимо также тщательно настроить параметры безопасности того программного и аппаратного обеспечения, которое непосредственно будет иметь доступ в сеть.

Система должна подвергаться периодической проверке антивирусными средствами (не реже чем раз в месяц) и другими средствами, обеспечивающими безопасность в системе (если таковые имеются). В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники района обязаны: приостановить работу на компьютере, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя отдела, владельца зараженных файлов, смежные отделы, использующие эти файлы в работе, а также соответствующий отдел информационных технологий, соответствующего специалиста по информационной безопасности.

Все внешние носители информации, полученные из сомнительных или неизвестных источников должны подвергаться полному антивирусному сканированию перед использованием.

Необходимо регулярно обновлять версии программного обеспечения, связанного с обеспечением безопасности системы; устанавливать официальные обновления программ, которые имеют прямое или косвенное отношение к работе с сетью. Сюда же относятся и обновления, связанные с управлением аппаратным обеспечением системы (драйверы устройств и т.п.).

При обнаружении зараженных вирусами данных, эти данные должны немедленно и безвозвратно удаляться. Исключение составляют лишь важные данные, для которых имеет смысл попробовать применить процедуры восстановления.

Следует с большой осторожностью относится к программам, в которых присутствуют определенного рода уязвимости для несанкционированного проникновения, или же в которых включены особые привилегии для их разработчиков.

Необходимо внимательно проанализировать систему данных сотрудника и обеспечить ее структурированное хранение на носителях информации. Все данные должны классифицироваться согласно их применению или же по-другому, четко установленному сотрудником критерию (например, критериями могут служить соображения конфиденциальности данных, место из размещения и способ пересылки).

## 10.Правила доступа в Интернет

Программное обеспечение, обеспечивающее защиту системы от проникновения, должно быть задействовано в полном объеме на протяжении всего сеанса связи с Интернетом.

Допускается временное отключение части программного обеспечения, обеспечивающего защиту системы, в тех случаях, когда без этого невозможно выполнить какой-либо вид работы. После выполнения данного вида работ отключенные части системы защиты должны быть вновь задействованы.

Сотрудники района допускаются к использованию Интернета только после прохождения инструктажа, в котором разъяснялась бы Политика безопасности данной системы в отношении глобальной сети.

Сотрудники района должны стараться предоставлять о себе как можно меньше информации в сеть, а тем более не должны разглашать любую конфиденциальную информацию.

Все файлы, полученные из Интернета, перед их использованием должны пройти дополнительную антивирусную проверку.

После каждого сеанса связи с Интернетом необходимо проводить очистку системы от ненужных служебных данных, которые появились в результате соединения с сетью.

Все данные, полученные из Интернета должны систематизироваться и сохраняться.

## 11.Правила безопасности электронной почты

Все наиболее важные сообщения электронной почты должны архивироваться, особенно те сообщения, которые присланы официальными группами технической поддержки каких-либо информационных ресурсов. Также регулярной архивации должна подвергаться информация, касающаяся данных о тех сотрудниках, с которыми осуществляется связь средствами электронной почты (адресные книги и т.д.).

Все ранее сохраненные почтовые сообщения, потерявшие свою актуальность, должны быть тщательным образом безвозвратно уничтожены со всех носителей информации.

Необходимо в обязательном порядке сканировать каждое исходящее и получаемое сообщение электронной почты на наличие потенциально опасного содержимого (вирусы, «черви» и т.д.). Почтовые сообщения, не

удовлетворяющие установленным требованиям, должны немедленно и безвозвратно удаляться.

Необходимо на всех используемых почтовых ящиках установить, при необходимости, ограничения на содержимое и размер принимаемых сообщений и отсеивать те сообщения, которые не удовлетворяют установленным критериям.

После отправки письма по электронной почте необходимо хранить его до тех пор, пока не будет уверенности (подтверждения) в том, что оно достигло получателя. Это же касается и любых других способов передачи информации. Все файлы (особенно исполнимые и файлы больших размеров), полученные вместе с сообщением электронной почты без какого-либо запроса со стороны сотрудника района (особенно от неизвестного адресата) должны немедленно и безвозвратно удаляться без оценки их полезности. При этом каждый подобный факт должен быть зарегистрирован. Если нет полной уверенности в необходимости удаления данного сообщения, необходимо, в случае если адресат известен и только в этом случае, дополнительно связаться с ним (не по электронной почте) и попросить у него подтверждения в посылке сообщения.

Сотрудники района не должны участвовать в рассылке посланий, передаваемых по цепочке, не должны отвечать на оскорбительные и провокационные сообщения. Такие послания должны быть сначала переданы службам технической поддержки используемых почтовых сервисов для анализа, а после этого – безвозвратно удалены из системы. Также необходимо принять все возможные меры по обеспечению прекращения получения из данного источника подобной информации в будущем.

## 12.Правила управления доступом

В отношении всех основных и не основных (гости и проч.) сотрудников района необходимо осуществлять комплекс мер по обеспечению их работы в автоматизированной системе района, в частности регистрацию, выделение определенных информационных ресурсов и установление четких не избыточных, а только необходимых, прав доступа к ним.

Служба регистрации должна обеспечить положительную аутентификацию. Это даст гарантию того, что законный пользователь получит доступ к системе.

Необходимо в обязательном порядке регистрировать все удачные и неудачные попытки входа в систему, а также вести аудит доступа сотрудников района к ее объектам и периодически просматривать результаты его работы.

При первой же необходимости работы с системой при помощи удаленного доступа или же с локальной сетью необходимо разработать правила безопасности, регламентирующие данные виды работ.

Использование имен и паролей для доступа к информационным ресурсам:

необходимо использовать пароли везде, где это целесообразно;

следует придерживаться следующих правил составления и использования паролей - пароль должен состоять не менее чем из шести символов, состоять из произвольных комбинаций букв, цифр и других символов или же представлять

собой бессмысленную комбинацию слов, включающую буквы верхнего регистра;

необходимо менять все пароли не реже, чем раз в два месяца (желательно делать это не по графику), при этом использовать пароли повторно не разрешается;

запрещено использовать одинаковые пароли для доступа к разным информационным ресурсам;

пароли необходимо хранить в надежном, недоступном для посторонних месте или же использовать специальные аппаратные средства для их хранения;

хранение паролей осуществляется операционной системой, и установленный ею уровень защиты не может быть ослаблен;

запрещено сообщать свои пароли третьим лицам в какой бы то ни было форме;

пароли запрещается писать на компьютерных терминалах, помещать в общедоступные места;

необходимо заменить все пароли, назначенные системой по умолчанию, на собственные, а потом, если это возможно, отключить возможность доступа к данному ресурсу по стандартному паролю;

все имена и пароли для доступа к каким-либо информационным ресурсам, которые не используются, подлежат надежной блокировке;

система должна предотвращать попытки регистрации и перерегистрации тех сотрудников, чьи имена и пароли для входа в систему не соответствуют установленным правилам;

при получении доступа к какому-либо информационному ресурсу при помощи процесса авторизации по имени и паролю сотрудник не должен произносить эти данные вслух при вводе их в систему;

изменять пароли необходимо всякий раз, когда есть указания на возможную компрометацию систем или паролей.

## 13.Управление непрерывностью работы района

Основной целью управления непрерывностью работы района является противодействие прерывания работы и защита рабочих процессов от последствий при значительных сбоях или бедствиях.

Необходимо обеспечивать управление непрерывностью работы с целью минимизации отрицательных последствий, вызванных нарушениями безопасности. Последствия от нарушений безопасности и отказов в обслуживании необходимо анализировать, по результатам анализа разрабатывать и внедрять планы обеспечения непрерывности работы с целью восстановления рабочих процессов в течение требуемого времени при их нарушении. Такие планы следует поддерживать и применять на практике. Должна быть выработана стратегия непрерывности рабочего процесса в соответствии с согласованными целями и приоритетами. Необходимо чтобы планирование непрерывности работы начиналось с идентификации событий, которые могут быть причиной прерывания работы, например, отказ

оборудования, наводнение или пожар. Планирование должно сопровождаться оценкой рисков с целью определения последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления). Оценка риска должна распространяться на все рабочие процессы и не ограничиваться только средствами обработки информации. В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности работы. Разработанный план должен быть утвержден руководством района. Необходимо, чтобы план обеспечения непрерывности работы предусматривал следующие мероприятия по обеспечению информационной безопасности:

определение и согласование всех обязанностей должностных лиц и процедур на случай чрезвычайных ситуаций;

внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления рабочего процесса в течение требуемого времени;

особое влияние следует уделять оценке зависимости работы от внешних факторов и существующих контрактов;

документирование согласованных процедур и процессов;

соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление.

Необходимо, чтобы план обеспечения непрерывности работы соответствовал требуемым целям работы.

## 14.Ответственность за нарушение политики безопасности

Все сотрудники района несут ответственность за нарушение требований настоящей Политики информационной безопасности согласно действующему законодательству в области защиты информации.

## 15.Сопровождение правил

Все без исключения положения данного документа имеют одинаково равную силу и должны неукоснительно соблюдаться.

Политика информационной безопасности должна в обязательном порядке периодически перечитываться и пересматриваться (не реже чем один раз в год).

Ежемесячно должна проводиться оценка текущего состояния имеющихся у сотрудников информационных ресурсов. В результате этой оценки в соответствующие документы по безопасности должны вноситься необходимые изменения (если они есть).

При проведении каких-либо изменений в данных правилах, соответствующие изменения, при необходимости, должны производиться и в других документах, касающихся обеспечения безопасности.

Если возникли непредвиденные обстоятельства, требующие срочного пересмотра Политики информационной безопасности, то такой пересмотр может быть осуществлен до планового пересмотра.

При возникновении серьезных проблем с безопасностью системы (например, при успешном взломе системы безопасности) возникшая проблема должна быть немедленно проанализирована, а организационно-распорядительные документы по информационной безопасности – пересмотрены в соответствии с проведенным анализом. При этом нужно рассматривать проблему в целом и излишне не фокусировать внимание на отдельных деталях.

Копия настоящей Политики должна находиться в доступном для сотрудников района месте.

Приложение №4
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2021 № 221

**Положение**
**об обработке персональных данных Исполнительного комитета Актанышского муниципального района Республики Татарстан**

Настоящее Положение в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 2 марта 2007 года № 25-ФЗ «О муниципальной службе в Российской Федерации» устанавливает порядок получения, хранения, комбинирования, передачи и иного использования (далее – обработка) документов, содержащих сведения, отнесенные к персональным данным муниципальных служащих и иных работников Исполнительного комитета Актанышского муниципального района Республики Татарстан (далее – работники).

## I. Состав персональных данных работника

1.1. К документам, содержащим информацию персонального характера, относятся следующие документы и их комплексы:

1) документы, удостоверяющие личность работника или содержащие сведения о работнике:

паспорт гражданина Российской Федерации (временное удостоверение личности гражданина Российской Федерации, выдаваемого на период оформления паспорта в порядке, утверждаемом уполномоченным федеральным органом исполнительной власти);

военный билет;

страховое свидетельство обязательного пенсионного страхования;

документы об образовании (аттестаты, дипломы, свидетельства, сертификаты);

трудовая книжка;

медицинские справки и заключения;

свидетельство о присвоении ИНН;

2) учётные документы по личному составу:

личная карточка форма №№ Т-2, Т-2МС;

личное дело муниципального служащего;

вспомогательные регистрационно-учетные формы (книги, журналы, картотеки, базы данных), содержащие сведения персонального характера (журнал (книга) регистрации распоряжений по личному составу, книга учёта движения трудовых книжек и вкладышей к ним, журнал учёта отпусков, журнал учёта выдачи справок с места работы работника);

3) трудовые договоры (контракты), соглашения об изменении (дополнении) трудовых договоров (контрактов), договоры о материальной ответственности;

4) распорядительные документы по личному составу (подлинники и копии):

муниципальные правовые акты о приеме (заключении трудового договора (контракта)), переводе, увольнении (прекращении трудового договора, расторжении контракта);

муниципальные правовые акты о предоставлении отпуска, поощрении, взыскании;

5) документы об оценке деловых и профессиональных качеств работника при приёме на работу и в процессе работы (тесты, анкеты, резюме и т.д.);

6) документы, отражающие деятельность аттестационных и конкурсных комиссий (протоколы заседаний, аттестационные листы, решения, представления и др.);

7) документы, отражающие результаты служебных расследований и (или) рассмотрение вопроса о привлечении работника к дисциплинарной ответственности (докладные и объяснительные записки, акты, справки, протоколы и др.);

8) копии отчётов, иных документов, направляемых в государственные органы статистики, налоговые инспекции и другие организации;

9) документы бухгалтерского учёта, содержащие информацию о расчётах с персоналом (лицевые счёта, расчётно-платёжные ведомости, платёжные ведомости и т.д.);

10) сведения о доходах, об имуществе и обязательствах имущественного характера, предоставляемые гражданином при поступлении на муниципальную службу, а также сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, предоставляемые муниципальным служащим.

1.2. Если персональные данные работника содержатся в иных документах, на них распространяется действие настоящего Положения.

## II. Обязанности работодателя

2.1. В соответствии с законодательством в целях обеспечения прав и свобод человека и гражданина работодатель (его представители) при обработке персональных данных работника обязаны:

1) осуществлять обработку персональных данных работника исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе (работе), обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объёма и содержания обрабатываемых персональных данных работника руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля

2006 года № 152-ФЗ «О персональных данных» и иными федеральными законами;

3) получать все персональные данные работника у него самого. Возможно получение персональных данных у третьей стороны в случаях и порядке, установленных Трудовым кодексом Российской Федерации, иными федеральными законами и настоящим Положением;

4) обеспечить за счёт средств работодателя в порядке, установленном Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными федеральными законами защиту персональных данных работника от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

5) совместно с работниками и их представителями вырабатывать меры защиты персональных данных работников;

6)иные обязанности, установленные Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными федеральными законами.

2.2. В соответствии с законодательством в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника не вправе:

1) получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации работодатель (его представители) вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

2) получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

3) при принятии решений, затрагивающих интересы работника, основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.3. В соответствии с законодательством при передаче персональных данных работника работодатель обязан:

1) не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

2) не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

3) предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они

сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;

4) осуществлять передачу персональных данных работника в пределах Исполнительного комитета Актанышского муниципального района в соответствии с настоящим Положением, с которым работник должен быть ознакомлен под роспись;

5) разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

6) не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

7) передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации или иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

## III. Права и обязанности работника

3.1. В соответствии с законодательством в целях обеспечения защиты персональных данных, хранящихся у работодателя, работник имеет право на:

1) полную информацию об его персональных данных и обработке этих данных;

2) свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

3) определение своих представителей для защиты своих персональных данных;

4) доступ к медицинской документации, отражающей состояние его здоровья, с помощью медицинского работника по его выбору;

5) требование об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника работник имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

6) требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

7) обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

3.2. В целях обеспечения требований законодательства при обработке персональных данных работника работник обязан:

1) передавать работодателю или его представителю достоверные персональные данные и документы, содержащие информацию персонального характера, в случаях и порядке, установленных Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», иными федеральными законами, настоящим Положением;

2) в срок, не превышающий 3 (трех) рабочих дней, сообщать работодателю или его представителю об изменении своих персональных данных.

3.3. Работник и (или) его представитель должны быть ознакомлены под роспись с настоящим Положением;

3.4. Работник не должен отказываться от своих прав на сохранение и защиту тайны персональных данных.

## IV. Обработка персональных данных работника

4.1. Все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работодатель (его представитель) обязан заранее уведомить об этом работника и получить от него письменное согласие. Работодатель (его представитель) должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.2. Обработка персональных данных работника работодателем (его представителем) возможна только с согласия работника либо без его согласия в случаях, предусмотренных в пункте 4.5 настоящего Положения.

4.3. Работодатель (его представитель) вправе обрабатывать персональные данные работника только с его письменного согласия.

4.4. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес работника (субъекта персональных данных), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя работника (субъекта персональных данных), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя работника (субъекта персональных данных);

3) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

7)срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

8) подпись субъекта персональных данных.

4.5. В соответствии с законодательством согласие работника не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации или иного федерального закона, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия работодателя;

2) обработка персональных данных в целях исполнения трудового договора (контракта), стороной которого является работник;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно;

5) в иных случаях, установленных федеральным законом.

4.6. В целях получения персональных данных работника при поступлении на работу работник заполняет анкету и автобиографию.

4.7. Анкета представляет собой перечень вопросов о персональных данных работника. Анкета заполняется работником самостоятельно. При заполнении анкеты работник должен заполнять все её графы, на все вопросы давать полные ответы, в строгом соответствии с записями, которые содержатся в его личных документах, не допускать исправлений или зачеркиваний, прочерков, помарок.

4.8. Автобиография представляет собой документ, содержащий описание в хронологической последовательности основных этапов жизни и деятельности принимаемого работника. Автобиография составляется в произвольной форме без помарок и исправлений.

4.9. Анкета и автобиография работника хранятся в личном деле работника.

4.10. Персональные данные работников хранятся на бумажных носителях в сейфе заместителя начальника организационного отдела (по кадрам) Исполнительного комитета Актанышского муниципального района Республики

Татарстан (далее – организационный отдел). Для этого используются специально оборудованные шкафы и сейфы, которые запираются и опечатываются. Персональные данные работников располагаются в алфавитном порядке. Ключ от шкафов и сейфов, в которых хранятся персональные данные работников, находится у заместителя начальника организационного отдела (по кадрам).

4.11. Конкретные обязанности по хранению персональных данных работников, заполнению, хранению документов, содержащих персональные данные работников, возлагаются на заместителя начальника организационного отдела и закрепляются в трудовом договоре, заключаемом с ним, и должностной инструкции.

4.12. Персональные данные работника могут также храниться на электронных носителях, доступ к которым должен быть ограничен многопользовательской системой с разграничением прав доступа.

4.13. Работодатель обеспечивает защиту персональных данных работников и ограничение доступа к персональным данным лицам, не уполномоченным законом либо работодателем для получения соответствующих сведений. Доступ к персональным данным работников осуществляется на основании письменного разрешения руководителя Исполнительного комитета Актанышского муниципального района Республики Татарстан (далее – Исполнительный комитет). В указанном разрешении указывается перечень персональных данных работника, к которым разрешается доступ и причина (необходимость) использования (получения) персональных данных работника.

4.14. Доступ к персональным данным работников без специального разрешения имеют:

1) руководитель Исполнительного комитета, его заместители;

2) начальник организационного отдела Исполнительного комитета;

3) заместитель начальника организационного отдела (по кадрам) Исполнительного комитета;

4) начальник и главный специалист отдела бухгалтерского учета и отчетности Исполнительного комитета;

5) начальник отдела информатизации и защиты информации Исполнительного комитета.

При получении персональных данных работника лица, указанные в настоящем пункте, имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, заданий.

4.15. Работодатель (его представитель) вправе предоставлять персональные данные работника третьей стороне только с письменного согласия работника, за исключением случаев, установленных федеральным законом и настоящим Положением.

4.16. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника, либо отсутствует письменное согласие работника на предоставление его

персональных сведений, работодатель (его представитель) обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

4.17. Персональные данные работников могут быть переданы их представителям в порядке, установленном Трудовым кодексом Российской Федерации, иными федеральными законами, в том объёме, в каком это необходимо для выполнения указанными представителями их функций.

4.18. Работодатель обеспечивает ведение журнала учёта выданных персональных данных работников, в котором регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана.

4.19. Передача персональных данных работников по телефону, факсу, электронной почте без письменного согласия работника на передачу в такой форме запрещается.

4.20. В целях обеспечения сохранности и конфиденциальности персональных данных работников все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только сотрудниками, имеющими доступ к работе с персональными данными в соответствии с их должностными инструкциями.

## V. Ответственность за нарушение порядка обработки персональных данных работника

Лица, виновные в нарушении норм, регулирующих обработку персональных данных работника, установленных Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», иными федеральными законами, настоящим Положением несут дисциплинарную, материальную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

Приложение №5
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2018 № ПР-221

**Перечень сведений конфиденциального характера**

1. Настоящий Перечень сведений конфиденциального характера (далее - Перечень) разработан в соответствии со статьей 139 Гражданского, кодекса Российской Федерации, Федеральным законом от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», на основании Перечня сведений конфиденциального характера, утвержденного Указом Президента Российской Федерации от 6 марта 1997г. №188, Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденного Постановлением Правительства Российской Федерации от 3 ноября 1994г. №1233, и нормативно- методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30 августа 2002г. №282, а также в соответствии с распоряжением Кабинета Министров Республики Татарстан от 16 июля 2007г. № 1011-р.

2. В настоящем Перечне под служебной тайной понимаются несекретные сведения, касающиеся деятельности исполнительного комитета Актанышского муниципального района (далее - Исполнительный комитет), ограничения на распространение которых, диктуются служебной необходимостью (служебная информация ограниченного распространения).

3. На носителях информации, содержащих сведения, отнесенные к служебной тайне, проставляется пометка «Для служебного пользования».

4. В настоящий перечень могут быть внесены дополнительные сведения, касающиеся сферы деятельности Исполнительного комитета.

# Перечень сведений конфиденциального характера

| № п/п | Наименование сведений | Примечание |
|---|---|---|
| 1 | 2 | 3 |
| **1. Сведения по общим вопросам организации деятельности в исполнительном комитете Актанышского муниципального района** | | |
| 1.1 | Сведения о содержании разрабатываемых исполнительным комитетом проектах постановлений и распоряжений, договоров и соглашений, методических документов | |
| 1.2 | Сведения о предложениях исполнительного комитета в проекты федеральных законов, межправительственных договоров и соглашений, указов, распоряжений Президента Российской Федерации, постановлений, распоряжений Правительства Российской Федерации, Республики Татарстан | |
| 1.3 | Сведения, содержащиеся в документах по вопросам организации взаимодействия исполнительного комитета с другими органами государственной власти | |
| 1.4 | Сведения о номерах правительственной, закрытой, специальной, служебной, факсимильной, мобильной связи, используемых руководством исполнительного комитета | |
| 1.5 | Сведения, раскрывающие отдельные вопросы организации, состояния пропускного или внутри объектового режима в исполнительном комитете | |
| 1.6 | Сведения об организации, состоянии, расположении инженерных систем, систем видеонаблюдения, пожарной, охранной сигнализации территорий, зданий, помещений исполнительного комитета | |
| 1.7 | Сведения, содержащиеся в заключениях о фактической осведомленности в сведениях, составляющих государственную тайну, специалиста исполнительного комитета, в том числе уволенного, если указанные сведения не содержат конкретных обоснований | |
| 1.8 | Сводные отчетные данные о практике применения исполнительного комитета законодательства об административных правонарушениях Российской Федерации | |
| 1.9 | Перечень сведений, отнесенных к служебной тайне, исполнительного комитета | |
| **2. Сведения по вопросам технической защиты информации** | | |
| 2.1 | Сведения об организации или фактическом состоянии защиты служебной информации ограниченного распространения в исполнительном комитете | |
| 2.2 | Рекомендации по вопросам технической защиты служебной информации ограниченного распространения в | |

| | | |
|---|---|---|
| | исполнительном комитете | |
| 2.3 | Сведения об организации и содержании проводимых мероприятий по технической защите служебной информации ограниченного распространения в исполнительном комитете | |
| 2.4 | Сведения, содержащиеся в планах проведения мероприятий по технической защите служебной информации ограниченного распространения в исполнительном комитете | |
| 2.5 | Сведения, содержащиеся в требованиях по технической защите служебной информации ограниченного распространения и (или) о мерах по их выполнению в исполнительном комитете | |
| 2.6 | Сведения, содержащиеся в первичных материалах контроля эффективности технической защиты служебной информации ограниченного распространения в исполнительном комитете | |
| 2.7 | Сведения, содержащиеся в материалах по аттестации объектов информатизации исполнительного комитета по требованиям безопасности информации | |
| **3. Сведения по бухгалтерским и кадровым вопросам** | | |
| 3.1 | Сведения о персональных данных сотрудника в исполнительном комитете: его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативными правовыми актами как защищаемая | |
| 3.2 | Сведения о начисленных доходах специалистов в исполнительном комитете | |

Приложение №6
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 16.05.2018 № 09-24

**Положение**
**о специалисте по информационной безопасности**

**1. Общие положения**

1.1. Настоящее Положение о специалисте по информационной безопасности (далее - Положение) определяет основные цели, функции и права специалиста по информационной безопасности в исполнительном комитете Актанышского муниципального района (далее - исполнительный комитет).

1.2. Специалист по информационной безопасности назначается постановлением руководителя исполнительного комитета на основании Положения о государственной системе зашиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993г. № 912-51.

1.3. Специалист по информационной безопасности проводит свою работу согласно нормативно-методическим документам Федеральной службы по техническому и экспортному контролю (Гостехкомиссии России).

1.4. Непосредственное руководство работой специалиста по информационной безопасности осуществляет руководитель исполнительного комитета.

1.5. Назначение и освобождение от должности специалиста по информационной безопасности производится руководителем исполнительного комитета. Примечание: специалист по информационной безопасности (защите информации) может быть назначен, по усмотрению руководителя исполнительного комитета, из числа сотрудников одного из подразделений исполнительного комитета, имеющих опыт работы по основной деятельности исполнительного комитета или в области защиты информации и отвечающих требованиям квалификационных характеристик на специалистов по комплексной защите информации.

1.6. Специалист по информационной безопасности проводит свою работу во взаимодействии с соответствующими режимно-секретными подразделениями исполнительного комитета, отделом информационной безопасности Министерства информатизации и связи Республики Татарстан,

Федеральной службой безопасности России, Федеральной службой по техническому и экспортному контролю России и другими министерствами и ведомствами.

1.7. Работа специалиста по информационной безопасности проводится в соответствии с планами работ.

1.8. На специалиста по информационной безопасности запрещается возлагать иные, несвязанные с его основной деятельностью, обязанности.

1.9. В своей работе специалист по информационной безопасности руководствуется законодательными и иными нормативными актами Российской Федерации, Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, решениями Федеральной службы по техническому и экспортному контролю (Гостехкомиссии России), постановлениями и распоряжениями руководителя исполкома и другими руководящими документами по защите информации и противодействию техническим средствам разведки.

## 2. Основные функции специалиста по информационной безопасности

Основными функциями специалиста по информационной безопасности являются:

2.1. Проведение единой технической политики, организация и координация работ по защите информации в исполнительном комитете.

2.2. Осуществление планирования работ по защите информации от иностранных технических разведок и от ее утечки по техническим каналам.

2.3. Участие в подготовке объектов исполнительного комитета к аттестации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

2.4. Разработка нормативно-методических документов по защите информации в исполнительном комитете.

2.5. Разработка (самостоятельно или совместно с режимно-секретными или другими подразделениями) проектов распорядительных документов по вопросам организации защиты информации в исполнительном комитете.

2.6. Организация в установленном порядке расследования причин и условий появления нарушений в области зашиты информации и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.7. Разработка предложений, участие в проводимых работах по совершенствованию системы защиты информации исполнительного комитета.

2.8. Подготовка рекомендаций по перечню подведомственных предприятий, учреждений и организаций, которые подлежат лицензированию на право проведения мероприятий и (или) оказания услуг в области защиты информации.

2.9. Организация и координация разработки, внедрения и эксплуатации системы мер по безопасности информации, обрабатываемой техническими средствами в целях предотвращения утечки информации по техническим каналам.

2.10. Разработка (самостоятельно или совместно с режимно-секретными или другими подразделениями) комплекса мероприятий по защите информации при установлении и осуществлении научно-технических и торгово-экономических связей с зарубежными организациями, а также при посещении исполнительного комитета иностранными представителями.

2.11. Участие в согласовании технических заданий на проведение работ, содержащих сведения, отнесенные к государственной или служебной тайне.

2.12. Проведение периодического контроля эффективности мер защиты информации в исполнительном комитете.

2.13. Учет и анализ результатов контроля.

2.14. Организация повышения осведомленности по вопросам защиты информации руководства и сотрудников исполнительного комитета.

2.15. Подготовка отчетов о состоянии работ по защите информации в исполнительном комитете.

## 3. Права специалиста по информационной безопасности

Специалист по информационной безопасности имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам защиты информации.

3.2. Разрабатывать проекты организационных и распорядительных документов по защите информации.

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

3.4. Контролировать деятельность структурных подразделений исполнительного комитета в части выполнения ими требований по защите информации.

3.5. Участвовать в работе постоянно действующей технической комиссии исполнительного комитета при рассмотрении вопросов по защите информации.

3.6. Вносить предложения руководителю исполнительного комитета о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) информации, содержащей сведения, отнесенные к государственной или служебной тайне.

3.7. Привлекать в установленном порядке необходимых специалистов из числа сотрудников исполнительного комитета для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам защиты информации.

## 4. Ответственность специалиста по информационной безопасности

Специалист по информационной безопасности несет персональную ответственность за: соответствие визируемых им документов, представляемых на подпись руководству исполнительного комитета; правильность и объективность принимаемых решений; правильное и своевременное выполнение приказов, распоряжений, указаний руководства исполнительного комитета по вопросам, входящим в возложенные на него функции; выполнение возложенных на него обязанностей, предусмотренных настоящим Положением; соблюдение трудовой дисциплины, охраны труда; реализацию принятой в исполнительном комитете политики информационной безопасности; качество проводимых работ по обеспечению защиты информации в соответствии с функциональными обязанностями; согласно действующему законодательству Российской Федерации за разглашение сведений, составляющих государственную, служебную или иную тайну, и сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение №7
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2018 № 01-05/241

# ПОЛОЖЕНИЕ
## о категорировании информационных ресурсов

### 1. Общие положения

1.1. Настоящим Положением о категорировании информационных ресурсов (далее - Положение) вводятся категории информационных ресурсов и устанавливается порядок категорирования информационных ресурсов автоматизированных систем (далее - АС) исполнительного комитета Актанышского муниципального района (далее - Исполнительный комитет), подлежащих защите. Согласно руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденному решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года, для проведения классификации АС Исполнительного комитета необходимы следующие исходные данные: перечень защищаемых информационных ресурсов АС Исполнительного комитета, подлежащих защите и уровень их конфиденциальности; перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий; матрица доступа или полномочий субъектов доступа по отношению к информационным ресурсам АС, подлежащих защите.

1.2. Категорирование информационных ресурсов АС является необходимым элементом организации работ по обеспечению информационной безопасности Исполнительного комитета и имеет цели:

создание основы для классификации АС Исполнительного комитета;

типизацию принимаемых организационных мер и распределения аппаратно-программных средств защиты информационных ресурсов по рабочим станциям (далее - РС) и серверам АС Исполнительного комитета и унификацию вариантов настроек средств защиты.

### 2. Категории защищаемой информации

2.1. Исходя из необходимости обеспечения различных уровней защиты разных видов информации (не содержащей сведений, составляющих государственную тайну), хранимой и обрабатываемой в АС Исполнительного комитета, а также с учетом возможных путей нанесения ущерба Исполнительному комитету вводятся три категории конфиденциальности защищаемой информации.

2.2. Категории конфиденциальности защищаемой информации:

*«Строго конфиденциальная»* - к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства, а также информация, ограничения на распространение которой введены решениями руководства Исполнительного комитета, разглашение которой может привести к нанесению тяжкого ущерба Исполнительному комитету;

*«Конфиденциальная»* - к данной категории относится информация, не отнесенная к категории «Строго конфиденциальная», ограничения на распространение которой вводятся решением руководства Исполнительного комитета в соответствии с предоставленными ему как собственнику либо уполномоченному собственником лицу информации действующим законодательством правами, разглашение которой может привести к нанесению ощутимого ущерба Исполнительному комитету;

*«Открытая»* - к данной категории относится информация, обеспечения конфиденциальности которой не требуется.

2.3. Виды тайн:

адвокатская тайна (Федеральный закон РФ от 31.05.2002 № 63-ФЭ «Об адвокатской деятельности и адвокатуре в Российской Федерации»);

банковская тайна (Федеральный закон РФ от 02.12.1990 № 395-1 «О банках и банковской деятельности» (с изменениями от 29 июля 2004г.));

врачебная тайна («Основы законодательства Российской Федерации об охране здоровья граждан» от 22 июля 1993г. № 5487-1 (с изменениями от 22 августа 2004г.));

персональные данные, личная и семейная тайна («Перечень сведений конфиденциального характера» (утвержден Указом Президента РФ от 6 марта 1997г. № 188));

служебная и коммерческая тайна («Перечень сведений конфиденциального характера» (утвержден Указом Президента РФ от 6 марта 1997г. № 188);

тайна связи (Федеральный закон РФ от 07.07.2003 № 126-ФЗ «О связи»);

тайна следствия и судопроизводства («Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ);

тайна совещания судей («Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ).

## 3. Порядок определения категорий защищаемых информационных ресурсов АС

3.1. Категорирование информационных ресурсов АС проводится на основе их инвентаризации согласно методике категорирования защищаемых информационных ресурсов (приложение №1 к настоящему Положению) и предполагает составление и последующее ведение, поддержание в актуальном состоянии перечня информационных ресурсов АС, подлежащих защите (приложение №2 к настоящему Положению).

3.2. Ответственность за составление и ведение перечня информационных ресурсов АС, подлежащих защите (приложение №2 к настоящему Положению), перечня лиц, имеющих доступ к штатным средствам АС (приложение №3 к настоящему Положению), с указанием их уровня полномочий, и матрицы доступа или полномочий субъектов доступа по отношению к информационным ресурсам АС, подлежащим защите, (приложение №4 к настоящему Положению) Исполнительного комитета возлагается: в части составления и ведения перечней и матрицы доступа - на специалиста Исполнительного комитета, обслуживающего информационный ресурс; в части определения требований к обеспечению конфиденциальности и присвоение соответствующих категорий информационным ресурсам - на соответствующие подразделения (специалистов) Исполнительного комитета, которые непосредственно работают с информационными ресурсами, и специалиста по информационной безопасности Исполнительного комитета.

3.3. Контроль за правильностью категорирования информационных ресурсов АС Исполнительного комитета осуществляется соответствующим специалистом по информационной безопасности Исполнительного комитета.

3.4. Категорирование информационных ресурсов АС Исполнительного комитета может осуществляться последовательно для каждой конкретной подсистемы АС в отдельности с последующим объединением и формированием единого перечня информационных ресурсов АС Исполнительного комитета, подлежащих защите.

3.5. Изменение категории информационных ресурсов АС Исполнительного комитета производится при изменении требований к обеспечению защиты свойств конфиденциальности соответствующей информации.

3.6. Периодически (раз в год) или по требованию руководителей структурных подразделений Исполнительного комитета, использующих АС,

производится пересмотр установленных категорий защищаемых информационных ресурсов АС Исполнительного комитета на предмет их соответствия реальному положению дел.

## 4. Порядок пересмотра положения

4.1. В случае внесения изменений и дополнений в перечень информационных ресурсов, подлежащих защите, пересмотру с последующим утверждением подлежит приложение №2 к данному Положению.

4.2. Любой пересмотр настоящего Положения должен осуществляться на основании решения руководства Исполнительного комитета.

Приложение 1
к Положению о категорировании
информационных ресурсов

**Методика категорирования**
**защищаемых информационных ресурсов**

1. Настоящая методика уточняет порядок проведения работ по категорированию информационных ресурсов АС Исполнительного комитета, подлежащих защите, в соответствии с Положением о категорировании информационных ресурсов.

2. Категорирование предполагает проведение работ по выявлению и анализу всех информационных ресурсов подсистем АС Исполнительного комитета, подлежащих защите.

3. Для проведения анализа всех подсистем АС Исполнительного комитета и проведения инвентаризации информационных ресурсов АС, подлежащих защите, формируется специальная рабочая группа. В состав этой группы включаются соответствующие специалисты информационных технологий, информационной безопасности и других подразделений Исполнительного комитета (осведомленные в вопросах технологии автоматизированной обработки информации в АС Исполнительного комитета). Для придания необходимого статуса рабочей группе издается соответствующее распоряжение руководства Исполнительного комитета, в котором, в частности, даются указания всем начальникам структурных подразделений Исполнительного комитета об оказании содействия и необходимой помощи рабочей группе в проведении работ по анализу информационных ресурсов всех АС Исполнительного комитета. Для оказания помощи на время работы группы в подразделениях начальниками этих подразделений должны выделяться сотрудники, владеющие детальной информацией по вопросам обработки информации в данных подразделениях.

4. В ходе обследования конкретных подразделений Исполнительного комитета и автоматизированных подсистем выявляются все виды информационных ресурсов, используемых при решении задач в подразделениях Исполнительного комитета.

5. Все выявленные в ходе обследования информационные ресурсы заносятся в перечень информационных ресурсов, подлежащих защите (приложение №2 к Положению о категорировании информационных ресурсов).

6. Далее определяется и затем указывается в перечне информационных ресурсов, подлежащих защите, категория конфиденциальности и к какому типу

тайны относится каждый из выявленных информационных ресурсов на основании требований действующего законодательства и предоставляемых Исполнительному комитету прав.

7. Первоначальные предложения по оценке категории обеспечения конфиденциальности конкретных видов информации выясняются у руководителей соответствующих структурных подразделений Исполнительного комитета. Данные оценки категории информации заносятся в перечень информационных ресурсов, подлежащих защите (в колонку 2). Размещение информационного ресурса АС Исполнительного комитета выясняется у соответствующего сотрудника отдела информационных технологий (специалиста) Исполнительного комитета.

8. В дальнейшем с участием ответственных специалистов Исполнительного комитета необходимо уточнить и внести в приложение №3 к Положению о категорировании информационных ресурсов сведения о пользователях и их уровне доступа к штатным средствам АС Исполнительного комитета.

9. На следующем этапе составляется матрица доступа или полномочий субъектов доступа по отношению информационным ресурсам АС, подлежащим защите (приложение №4 к Положению о категорировании информационных ресурсов).

10. На последнем этапе определяется класс АС на основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Исходя из класса АС определяются типовые конфигурации принимаемых мер и настройки защитных механизмов программно-аппаратных средств защиты информации.

Приложение 2
к Положению о категорировании
информационных ресурсов

**ПЕРЕЧЕНЬ***
**информационных ресурсов АС Исполнительного комитета,**
**подлежащих защите**

| № п/п | Наименование информационного ресурса (информации) | Категория конфиденциальности и вид тайны | Размещение ресурса (РС, устройство, каталог, файл) | Ответственный (подразделение) за определение требований к защищенности ресурса |
|---|---|---|---|---|
| | | | | |
| | | | | |

* Утверждается руководителем исполнительного комитета

Приложение 3
к Положению о категорировании
информационных ресурсов

**ПЕРЕЧЕНЬ***

**лиц, имеющих доступ к штатным средствам АС**

| № п/п | Наименование штатных средств | ФИО, должность лица, имеющего доступ | Уровень доступа к штатным средствам |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

* Утверждается руководителем исполнительного комитета

Приложение 4
к Положению о категорировании
информационных ресурсов

**МАТРИЦА***
**ДОСТУПА ИЛИ ПОЛНОМОЧИЙ СУБЪЕКТОВ ДОСТУПА**
**по отношению к информационным ресурсам АС, подлежащим защите**

| № п/п | Помещение (каб.№) | АРМ № | Имя АРМ в домене hq.mcrt.ru | IP адрес | Имя пользователя | Подсистемы/ Задачи | Ф.И.О. пользователя | Категория доступа | Номер пункта из Перечня | Подразделение |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |

* Утверждается руководителем исполнительного комитета

Приложение № 8
К постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2018 № 1[illegible]

**Регламент доступа**
**в помещения с серверным и телекоммуникационным оборудованием**

1. Помещения с серверным и телекоммуникационным оборудованием (далее - серверные помещения) Исполнительного комитета Актанышского муниципального района (далее - Исполнительный комитет) относятся к помещениям с ограниченным доступом.

2. К серверным помещениям Исполнительного комитета относятся помещения, где установлено серверное и телекоммуникационное оборудование исполнительного комитета.

3. Серверные помещения должны быть оснащены охлаждающим оборудованием, средствами контроля доступа и охранной сигнализацией. Оснащение серверных помещений должно соответствовать правилам техники безопасности, санитарным нормам, отвечать требованиям пожарной безопасности, исключать возможность бесконтрольного проникновения в него посторонних лиц, гарантировать сохранность находящегося в нем имущества, работоспособность серверного и коммутационного оборудования.

4. Входные двери в серверные помещения должны быть прочными (рекомендуется установка металлических дверей) и должны быть оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время.

5. В серверные помещения допускаются лица, которые имеют прямое отношение к проводимым в этих помещениях работам, а также лица, осуществляющие контроль за проведение работ. Перечень таких лиц утверждается распоряжением руководителя исполнительного комитета приложение №1 к настоящему регламенту. Доступ других лиц в серверное помещение может быть разрешен лишь в случае служебной необходимости руководителем исполкома и фиксируется в «Журнале контроля допуска в серверное помещение» (приложение №2 к настоящему регламенту).

6. Все работы, проводимые на серверном или коммутационном оборудовании, хозяйственные, ремонтные работы, в том числе уборка могут проводиться лишь в присутствии лиц, указанных в приложении №1 к настоящему Регламенту и фиксируются в «Журнале контроля допуска в серверное помещение».

7. Серверные помещения должны быть в установленном порядке обеспечены первичными и исправными средствами пожаротушения и пожарной сигнализацией. Каждый работник в соответствии с перечнем лиц, указанных в приложении №1 к настоящему Регламенту, обязан уметь пользоваться первичными средствами пожаротушения. Ответственный за противопожарное состояние серверных помещений исполнительного комитета должен ежедневно проводить их осмотр, своевременно проверять годность огнетушителей.

8. При пожаре, аварии или стихийном бедствии сотрудник охраны (дежурный) Исполнительного комитета немедленно вызывает пожарную команду или аварийно-спасательную службу, ставит в известность ответственного за противопожарное состояние серверных помещений Исполнительного комитета, руководителя Исполнительного комитета. В случае чрезвычайных ситуаций коммутационные шкафы, отдельные серверы отсоединяются от сетей и выносятся из серверного помещения в безопасное место сотрудниками исполнительного комитета совместно с сотрудниками охраны и аварийно-спасательных служб.

Приложение №1
к Регламенту доступа в помещения с
серверным и телекоммуникационным
оборудованием

**Список лиц,**
**допущенных в серверное помещение Исполнительного комитета**

| № п/п | ФИО | должность | отдел |
|---|---|---|---|
| | | | |
| | | | |

Приложение №2
к Регламенту доступа в помещения с
серверным и телекоммуникационным
оборудованием

**ЖУРНАЛ УЧЕТА РАБОТ В СЕРВЕРНОМ ПОМЕЩЕНИИ КОМ. №**
**Начат: «____» _____ г.**
**Окончен: «____»_____г.**
**Срок хранения _____**

| Дата | Время входа/ выхода | Ф.И.О. сотрудника, телефон | Наименование организации | Проведенные работы | Подпись сотрудника | Подпись ответственного за вход |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |

Приложение №9
к постановлению Руководителя
Исполнительного комитета
Актанышского муниципального
района от 06.09.2018 № ПР-221

# ПОЛОЖЕНИЕ
## о порядке обращения с информацией конфиденциального характера

### 1. Общие положения

1.1. Настоящее Положение о порядке обращения с информацией конфиденциального характера (далее - Положение) разработано в соответствии с Постановлением Правительства Российской Федерации от 3 ноября 1994г. №1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Федеральных органах исполнительной власти» и определяет общий порядок обращения с документами и другими материальными носителями (фото-, кино-, видео- и аудиопленки, машинные носители информации и др.) информации (далее - документами), содержащими конфиденциальную информацию, в Исполнительном комитете Актанышского муниципального района (далее - Исполнительный комитет).

1.2. К информации конфиденциального характера относится несекретная информация, касающаяся деятельности Исполнительного комитета, ограничения на распространение которой диктуются служебной необходимостью.

1.3. Не могут быть отнесены к информации конфиденциального характера: акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации; сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов; описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес; порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц; решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке; сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения; документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

1.4. На документах (в необходимых случаях и на проектах документов), содержащих информацию конфиденциального характера, проставляется пометка «Для служебного пользования».

1.5. Руководитель Исполнительного комитета в пределах своей компетенции определяет:

- категории должностных лиц, уполномоченных относить информацию к разряду конфиденциальной;
- порядок передачи информации конфиденциального характера другим органам и организациям;
- порядок снятия пометки «Для служебного пользования» с носителей информации конфиденциального характера;
- организацию защиты информации конфиденциального характера.

1.6. Должностные лица Исполнительного комитета, принявшие решение об отнесении информации к разряду конфиденциальной, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных пунктом 1.3 настоящего Положения.

1.7. Информация конфиденциального характера без санкции соответствующего должностного лица не подлежит разглашению (распространению).

1.8. За разглашение информации конфиденциального характера, а также нарушение порядка обращения с документами, содержащими такую информацию, государственные гражданские служащие и другие работники Исполнительного комитета могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности.

1.9. В случае ликвидации Исполнительного комитета решение о дальнейшем использовании информации конфиденциального характера принимает ликвидационная комиссия.

1.10. Ответственность за обеспечение правильного ведения, учета, хранения, размножения и использования документов, дел и изданий с пометкой «Для служебного пользования» возлагается в структурных подразделениях Исполнительного комитета на руководителей этих подразделений и их заместителей.

1.11. Контроль за правильной организацией этой работы, а также инструктаж лиц, ответственных за ведение делопроизводства по документам с пометкой «Для служебного пользования», возлагается на соответствующие структурные подразделения Исполнительного комитета, которым поручен прием и учет несекретной документации.

1.12. Контроль за неразглашением сведений, содержащихся в документах, делах и изданиях с пометкой «Для служебного пользования», осуществляется соответствующим отделом (штатным специалистом) Исполнительного комитета, ответственным за информационную безопасность Исполнительного комитета или на соответствующие структурные подразделения Исполнительного комитета, которым поручен прием и учет секретной документации.

1.13. Работники Исполнительного комитета, имеющие отношения к работе с документами, делами и изданиями «Для служебного пользования», должны в обязательном порядке ознакомиться с настоящим Положением.

**2. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения**

2.1. Необходимость проставления пометки «Для служебного пользования» на документах, содержащих информацию конфиденциального характера, определяется исполнителем, подписывающим, и руководителем Исполнительного комитета (заместителем), утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

2.2. Регистрация документов, содержащих информацию конфиденциального характера в Исполнительном комитете, осуществляется соответствующими структурными подразделениями Исполнительного комитета, которым поручен прием и учет несекретной документации.

2.3. Документы с пометкой «Для служебного пользования»:

- печатаются в подразделениях Исполнительного комитета. На обороте последнего листа каждого экземпляра документа должно быть указано количество отпечатанных экземпляров, фамилия исполнителя документа и дата печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации сотруднику соответствующего структурного подразделения Исполнительного комитета, которому поручен прием и учет несекретной документации. Черновики и варианты уничтожаются этим сотрудником с отражением факта уничтожения в учетных формах;
- учитываются, как правило, отдельно от несекретной документации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному индексу документа добавляется пометка «Для служебного пользования»;
- передаются работникам подразделений Исполнительного комитета под расписку;
- пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
- тиражируются только с письменного разрешения соответствующего руководителя подразделения Исполнительного комитета, где разрабатывался документ. Учет размноженных документов осуществляется поэкземплярно;
- хранятся в надежно запираемых и опечатываемых шкафах (хранилищах).

2.4. При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, готовившего документ.

2.5. Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое помещены такие документы, также проставляется пометка «Для служебного пользования».

2.6. Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

2.7. Передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения соответствующего руководителя подразделения Исполнительного комитета.

2.8. При смене работника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема-сдачи этих документов, который утверждается соответствующим руководителем подразделения Исполнительного комитета и подписывается ответственными, сдающим и принимающим ведение делопроизводства «Для служебного пользования» в данном подразделении.

2.9. Проверка наличия документов, дел и изданий с пометкой «Для служебного пользования» проводится не реже одного раза в год комиссиями, назначаемыми распоряжением руководителя Исполнительного комитета. В состав таких комиссий обязательно включаются работники, ответственные за учет и хранение этих материалов.

В библиотеках и архивах, где сосредоточено большое количество изданий, дел и других материалов с пометкой «Для служебного пользования», проверка наличия таких документов может проводиться не реже одного раза в пять лет.

Результаты проверки оформляются актом.

2.10. О фактах утраты документов, дел и изданий, содержащих информацию конфиденциального характера, либо разглашения этой информации ставится в известность руководителю Исполнительного комитета и назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю Исполнительного комитета, назначившему комиссию.

На утраченные документы, дела и издания с пометкой «Для служебного пользования» составляется акт, на основании которого делаются соответствующие отметки в учетных формах. Акты на утраченные дела постоянного срока хранения после их утверждения передаются в архив для включения в дело фонда.

2.11. При снятии пометки «Для служебного пользования» на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы направлялись.