



**Положение**  
о конфиденциальной информации

## **Общие положения**

- 1) Настоящее Положение регулирует в соответствии с Гражданским кодексом РФ, Федеральным законом РФ «Об информации, информационных технологиях и защите информации», иными федеральными законами и нормативными правовыми актами РФ отношения, связанные с охраной и использованием конфиденциальной информации ОГБУЗ ГБ г. Костромы (далее - Организация)
- 2) Конфиденциальная информация Организации - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления и существования, отнесенная к таковой в соответствии с настоящим Положением, имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам, ограничения к доступу и разглашению которой предпринимаются согласно нормам настоящего Положения.
- 3) Организация имеет исключительное право на использование конфиденциальной информации любыми незапрещенными законом способами по собственному усмотрению.
- 4) В соответствии с настоящим Положением Организация принимает меры к охране конфиденциальной информации и ограничению доступа к ней третьих лиц.
- 5) Целью охраны конфиденциальной информации является обеспечение экономической и правовой безопасности Организации.
- 6) Если, в связи с осуществлением своей деятельности, Организации становятся известны сведения, составляющие в соответствии с законодательством РФ защищаемую законом тайну, Организация обязана предпринимать меры по их охране в соответствии с нормативными правовыми актами о защищаемой законом тайне.
- 7) Действие настоящего Положения распространяется на все структурные подразделения Организации.
- 8) Настоящее Положение определяет единый режим конфиденциальности и является основным руководящим документом, обязательным для исполнения всеми Структурными подразделениями Организации.
- 9) В Организации могут применяться, при необходимости, средства и методы технической защиты конфиденциальной информации, а также другие меры, не противоречащие законодательству Российской Федерации.
- 10) Ответственность за организацию режима конфиденциальности в структурных подразделениях Организации несут их руководители и (или) ответственные лица.
- 11) Работники Организации несут ответственность за соблюдение режима конфиденциальности в соответствии с законодательством Российской Федерации и взятыми на себя добровольными обязательствами перед Организацией.

## **Охрана конфиденциальной информации Организации**

- 1) Охрана конфиденциальной информации Организации состоит в принятии комплекса мер, направленных на:
  - Ограничение доступа к конфиденциальной информации третьих лиц;
  - Предотвращение несанкционированного разглашения конфиденциальной информации;
  - Выявление и пресечение нарушений режима конфиденциальности информации;
  - Привлечение лиц, нарушающих режим конфиденциальности информации Организации к установленной ответственности.
- 2) Обязательным условием трудовых договоров, заключаемых с работниками Организации, является пункт о соблюдении работником конфиденциальной информации, которая может стать ему известной во время выполнения своих трудовых обязанностей в Организации.

- 3) Каждый сотрудник Организации при принятии на работу предупреждается под подпись об ответственности за нарушение конфиденциальности информации.
- 4) Руководители или ответственные лица структурных подразделений обязаны не реже одного раза в 2 года проводить среди непосредственно подчиненных им работников инструктаж по соблюдению режима конфиденциальности информации. Вновь принятый на работу сотрудник проходит инструктаж у Администратора информационной безопасности.
- 5) Данные о проведенном инструктаже фиксируются в журнале, который хранится у Администратора информационной безопасности.
- 6) Заключаемые Организацией, в лице любых уполномоченных лиц, договоры, должны содержать условие о сохранении контрагентами режима конфиденциальности.
- 7) В рабочих и иных помещениях Организации создаются условия, ограничивающие доступ к конфиденциальной информации третьих лиц и пресекающие несанкционированное разглашение конфиденциальной информации, в том числе устанавливаются технические средства защиты от несанкционированного доступа к информации.
- 8) Организация предпринимает меры по выявлению фактов нарушения режима защиты конфиденциальной информации путем проверок, мониторинга средств защиты и деятельности пользователей, использующих технические средства для обработки информации.
- 9) Организация предпринимает все допустимые законом способы по пресечению выявленных нарушений режима защиты конфиденциальной информации.
- 10) Лица, виновные в нарушении режима защиты конфиденциальной информации привлекаются к установленной локальными актами Организации и законом ответственности.

## **Порядок использования и предоставления конфиденциальной информации Организации**

- 1) Использование конфиденциальной информации Организации допускается только теми работниками Организации, которым доступ к такой информации необходим в силу выполняемых ими функций.
- 2) Предоставление конфиденциальной информации Организации третьим лицам возможно не иначе, как с согласия уполномоченных лиц Организации на разрешение подобных действий. Любое такое предоставление информации должно оформляться актом передачи или иного документа, подтверждающего факт передачи, основания передачи и цели такой передачи информации.
- 3) Иные случаи предоставления конфиденциальной информации предусмотрены действующим законодательством РФ.

## **Порядок отнесения информации к категории конфиденциальной**

- 1) Конфиденциальная информация Организации состоит из:
  - Сведений, составляющих коммерческую тайну;
  - Сведений, составляющих персональные данные работников и иных лиц, передавших свои персональные данные Организации в связи с деятельностью Организации.
- 2) К конфиденциальной информации следует относить:
  - Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность;
  - Сведения, составляющие охраняемую законодательством РФ тайну, переданную Организации установленным порядком;

- Техническую, технологическую, коммерческую, организационную или иную используемую в деятельности Организации информацию.

3) Не может быть отнесена к категории конфиденциальной информация:

- Содержащаяся в Едином государственном реестре юридических лиц, положениях о филиалах и представительствах юридических лиц;
- Содержащаяся в свидетельствах о регистрации гражданина в качестве индивидуального предпринимателя, лицензиях и иных документах на право занятия отдельными видами деятельности;
- В составе федерального имущества и об использовании средств федерального бюджета, о составе имущества и об использовании средств бюджетов субъектов Российской Федерации, о составе муниципального имущества и об использовании средств муниципальных бюджетов;
- О состоянии экологии, противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и о других факторах, влияющих на обеспечение безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- О численности, составе, об условиях труда работников и о наличии свободных рабочих мест;
- О задолженности работодателей по выплате заработной платы и по другим выплатам социального характера;
- О нарушениях законодательства Российской Федерации и об их последствиях;
- Об условиях приватизации объектов государственной и муниципальной собственности, о составе участников приватизации и средствах, вложенных этими участниками при приватизации;
- О деятельности и об использовании средств и имущества благотворительных организаций, кроме случаев, предусмотренных федеральными законами;
- О перечне лиц, имеющих право без доверенности выступать от имени юридического лица (совершать сделки);
- Обязательность раскрытия которых или недопустимость ограничения доступа, к которым установлены федеральными законами.

4) Степень конфиденциальности сведений должна соответствовать тяжести ущерба, который может быть нанесен интересам Организации в финансово-экономической, научно-технической и иных областях ее деятельности, а так же деловой репутации Организации вследствие распространения указанных сведений.

5) Под ущербом понимаются расходы, которые Организации понесла или должна будет понести для восстановления нарушенного права, утраты или повреждение имущества, а также неполученные доходы, которые Организация получила бы при обычных условиях, если бы её право не было нарушено.

6) Документам Организации, содержащим конфиденциальную информацию, могут (если это необходимо) присваиваются следующие грифы конфиденциальности: Коммерческая тайна, Врачебная тайна, Персональные данные.

7) Необходимость присвоения документу грифа конфиденциальности определяется исполнителем. Контроль соответствия грифа конфиденциальности содержанию документа осуществляет руководитель структурного подразделения.

8) Грифы конфиденциальности могут не проставляться на документах бухгалтерского учета и отчетности, договорах, финансовых документах установленной формы и документах, содержащих персональные данные работников Организации.

9) Порядок учета, хранения и работы с указанными документами в подразделении определяются руководителем Организации с учетом требований режима конфиденциальности. Пересылка (передача) таких документов другим подразделениям Организации или сторонним организациям производится установленным данным

Положением порядком. При этом грифы конфиденциальности проставляются на сопроводительном письме.

## **Порядок допуска к конфиденциальной информации и документам**

1) Допуск работников структурных подразделений Организации к конфиденциальной информации осуществляется в соответствии с полномочиями его должности. Если сотруднику для выполнения рабочих функций нужен доступ к информации, но его должность не подразумевает такого допуска, допуск такого сотрудника производится в соответствии с приказом руководителя Организации.

2) Руководитель структурного подразделения несет персональную ответственность за подбор работников своего подразделения, допускаемых к конфиденциальной информации, и обязан обеспечить систематический контроль над тем, чтобы к указанной информации получали доступ только те лица, которым она необходима для выполнения своих функциональных обязанностей.

3) Допуск работников к конфиденциальной информации осуществляется только после подписания ими Трудового договора установленного образца с принятием работником индивидуальных обязательств.

4) Командированные сторонними организациями лица допускаются к конфиденциальной информации Организации на основе письменных разрешений руководителя, согласованных с Администратором безопасности, при наличии Соглашения о конфиденциальности между Организацией и командирующей Организацией, письменных запросов руководителей организаций, в которых работают командированные, с указанием целей получения конфиденциальной информации и перечня конкретных сведений, а также предписаний на выполнение заданий.

## **Обязанности лиц, допущенных к конфиденциальной информации**

1) Лица, допущенные к конфиденциальной информации, обязаны:

- Выполнять установленный в Организации режим конфиденциальности;
- Не разглашать конфиденциальную информацию Организации и (или) её контрагентов, и без их согласия не использовать ее для собственных нужд в период действия трудового договора, а также в течение трех лет после его окончания, если предусмотренным трудовым договором соглашением между работником и работодателем не установлен иной срок;

- Незамедлительно сообщать непосредственному руководителю о ставших известными ему фактах разглашения либо угрозе разглашения конфиденциальной информации Организации и (или) её контрагентов, незаконном получении или незаконном использовании третьими лицами конфиденциальной информации Организации и (или) её контрагентов;

- Возместить причиненные убытки, если он виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с исполнением им трудовых обязанностей;

- Передать Организации при прекращении трудового договора материальные носители с конфиденциальной информацией Организации и (или) её контрагентов, имеющиеся в их распоряжении.

2) Лицам, допущенным к конфиденциальным работам, документам, запрещается:

- Вести переговоры по конфиденциальным вопросам по незащищенным линиям связи, записывать и передавать (по сетям передачи данных общего пользования, телефону,

Интернет и т.п.) конфиденциальную информацию с помощью самодельных шифров, кодов или условностей; производить без разрешения Администратора безопасности звукозаписи по конфиденциальным вопросам;

- Использовать конфиденциальную информацию в открытой служебной переписке, докладах и выступлениях, в открытых статьях и других материалах, предназначенных для опубликования;
- Сообщать какую-либо информацию о проводимых конфиденциальных работах при обращении по личным вопросам, с жалобами, просьбами и предложениями в государственные органы и общественные организации;
- Сообщать в письмах и телеграммах, направляемых в другие организации по вопросам контрагентских отношений, данные о характере проводимых конфиденциальных работ;
- Производить без разрешения Администратора безопасности видео-, фото- и киносъемки в помещениях Организации, в которых производятся конфиденциальные работы или работы с конфиденциальной информацией.

## **Контроль исполнения режима конфиденциальности**

- 1) Контроль исполнения режима конфиденциальности в Организации осуществляется в целях изучения и оценки фактического состояния защищенности конфиденциальной информации, выявления недостатков и нарушений режима конфиденциальности, установления причин таких недостатков и нарушений, а также выработки предложений, направленных на их устранение и предотвращение в будущем.
- 2) Внеплановые проверки исполнения режима конфиденциальности проходят по запросу администратора безопасности на основании известных ему сведений о нарушении вышеназванного режима.
- 3) Контроль исполнения режима конфиденциальности осуществляет комиссия по информационной безопасности Организации.
- 4) Участие в проверке не должно приводить к необоснованному увеличению осведомленности членов комиссии в конфиденциальной информации.
- 5) Проверки проводятся в присутствии руководителей Структурных подразделений Организации, подлежащих проверке, или замещающих их лиц.
- 6) Проверяющие имеют право знакомиться со всеми документами, имеющими отношение к проверяемым вопросам, а также проводить беседы и консультации со специалистами и исполнителями, получать письменные объяснения, справки, отчеты по всем вопросам, входящим в компетенцию комиссии.
- 7) По результатам проверки составляется акт с отражением в нем состояния режима конфиденциальности, выявленных недостатков и нарушений, предложений по их устранению.
- 8) Структурное подразделение, в котором проводилась проверка, составляет план мероприятий по устранению выявленных недостатков и нарушений, а также реализации предложений, содержащихся в акте. План согласовывается с Администратором безопасности Организации.
- 9) Об устранении выявленных в результате проверки недостатков и нарушений в режиме конфиденциальности и реализации предложений, руководитель проверенного структурного подразделения Организации в установленные планом сроки сообщает Администратору безопасности Организации.

## **Проведение служебного расследования по фактам утраты (разглашения) конфиденциальных документов**

- 1) О фактах утраты конфиденциальных документов руководители структурных подразделений обязаны немедленно сообщить Администратору безопасности Организации, который проводит служебное расследование с целью выяснения обстоятельств их утраты, и поиску утраченных документов.
- 2) Администратор безопасности при проведении служебного расследования обязан:
  - Установить обстоятельства утраты конфиденциальных документов;
  - Установить лиц, виновных в утрате (разглашении);
  - Установить причины и условия, способствовавшие утрате (разглашению);
  - Выработать рекомендации по их устранению.
- 3) Администратор безопасности при проведении служебного расследования, имеет право:
  - Производить осмотр помещений Организации (сейфов, столов, шкафов, и т. д.), где могут находиться утраченные документы;
  - Проверять конфиденциальную документацию, журналы учета конфиденциальных документов;
  - Опрашивать работников Организации, виновных в утрате (разглашении), а также других работников Организации, которые могут оказать содействие в установлении обстоятельств происшедшего и получать от них письменные объяснения;
  - Привлекать других работников структурного подразделения, не заинтересованных в исходе дела, для проведения отдельных действий служебного расследования.
- 4) Служебное расследование должно проводиться в максимально короткие сроки (не более месяца со дня обнаружения факта утери/разглашения). В эти же сроки должно быть принято решение о привлечении виновных лиц к ответственности в установленном порядке.
- 5) В случаях, когда в течение данного срока утраченные конфиденциальные документы не обнаружены, поиск может быть прекращен. О прекращении поиска составляется мотивированное заключение, которое утверждается администратором безопасности.
- 6) Результаты всех мероприятий, проводимых в процессе служебного расследования, документируются.
- 7) Для уточнения степени конфиденциальности утерянной информации администратор безопасности может привлекать специалистов, имеющих отношение к информации и документам, по которым дается заключение о степени их конфиденциальности.
- 8) Степень конфиденциальности утраченных документов, поступивших из других организаций, определяется специалистами организаций, подготовивших документы.
- 9) По окончании служебного расследования администратор безопасности представляет руководителю Организации на утверждение заключение о результатах проведенного служебного расследования с письменными объяснениями лиц, которых опрашивали члены комиссии, актами проверок документации, помещений, сейфов и т. п. и другие документы, имеющие отношение к служебному расследованию.

## **Заключительные положения**

- 1) Лица виновные в нарушении режима защиты конфиденциальной информации Организации привлекаются в установленном порядке к уголовной, административной, дисциплинарной и гражданско-правовой ответственности.
- 2) Во всем, что не урегулировано настоящим Положением, применяются положения действующего законодательства РФ.