|  |  |
| --- | --- |
| **Про этот документ** Для целей иллюстрации – можно удалить перед подписанием | |
| * Данный документ является локальным нормативным актом, который устанавливает режим коммерческой тайны. | * Такой режим считается установленным после принятия мер, указанных в п. 3. |
| * Работодатель обязан ознакомить сотрудников с перечнем конфиденциальной информации и с данным Положением под подпись, а также создать сотруднику необходимые условия для соблюдения им установленного режима коммерческой тайны. | * Меры по охране конфиденциальности информации признаются разумно достаточными, если:  1. исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя; 2. обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны. |
| * Доступ сотрудника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями. | * Также трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации. |
| [www.buzko.legal](http://www.buzko.legal) | |

УТВЕРЖДЕНО

Приказом [Генерального директора] № [номер]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[00] [месяц] 202[●] г.

**ПОЛОЖЕНИЕ**

**О КОММЕРЧЕСКОЙ ТАЙНЕ**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Настоящее Положение («**Положение**») разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом № 98-ФЗ «О коммерческой тайне» от 29 июля 2004 г. («**Закон о коммерческой тайне**») и иными нормативными правовыми актами Российской Федерации для урегулирования отношений, связанных с установлением, изменением и прекращением режима коммерческой тайны в [ООО «наименование юридического лица»] (ОГРН: [номер]) («**Организация**») в отношении информации, составляющей секрет производства (ноу-хау), а также любой иной информации, на которую в соответствии с договором или законом будет распространено действие данного Положения.
   2. Определения, употребляемые в настоящем Положении:
      1. «**Конфиденциальная информация»** имеет значение, указанное в пункте 2.1. Положения;
      2. «**Обладатель конфиденциальной информации**» – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;
      3. «**Разглашение конфиденциальной информации**» – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору;
      4. «**Сотрудник**» – работник Организации, устроенный по трудовому договору, или третьи лица (физические или юридические), с которыми у Организации заключен гражданско-правовой договор. Настоящее Положение распространяется на таких третьих лиц в той степени, в какой такие лица добровольно приняли на себя обязательство исполнять настоящее Положение.
   3. В целях охраны Конфиденциальной информации Организация обязана:
      1. Ознакомить под расписку Сотрудника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются Организация и ее контрагенты;
      2. Ознакомить под расписку Сотрудника с установленным Организацией режимом коммерческой тайны и с мерами ответственности за его нарушение;
      3. Создать Сотруднику необходимые условия для соблюдения им режима коммерческой тайны.
   4. В целях охраны конфиденциальности информации Организации Сотрудник обязан:
      1. Выполнять установленный Организацией режим коммерческой тайны;
      2. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются Организация и ее контрагенты, и без их согласия не использовать эту информацию в личных целях.
      3. Передать Организации при прекращении или расторжении трудового договора имеющиеся в пользовании сотрудника материальные носители информации, содержащие информацию, составляющую коммерческую тайну, либо уничтожить такую информацию или удалить ее с этих материальных носителей под контролем Организации.
      4. Немедленно сообщать своему непосредственному руководителю или его замещающему лицу об утрате или недостаче документов, содержащих конфиденциальную информацию, ключей от сейфов (хранилища), печатей, удостоверений, пропусков и т.п.
   5. Ответственным за обеспечение конфиденциальности информации в Организации является руководитель Организации.
   6. На документе или ином носителе, содержащем конфиденциальную информацию, проставляется гриф «Коммерческая тайна» с указанием даты, фамилии и подписи лица, поставившего гриф. Отсутствие такого грифа само по себе не означат, что соответствующая информация не является конфиденциальной информацией при условии, что сотрудник или иное третье лицо уведомлено о конфиденциальном характере информации иным образом.
2. **ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ**
   1. Конфиденциальной информацией Организации является информация, включая документы Организации, имеющая отношение к ее деятельности, которая имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, в том числе («**Конфиденциальная информация**»):
      1. Любая информация, включая, без ограничений, предложения, инструкции, договоры, исследовательские материалы, формулы, процессы, данные об используемой технологии, рынках сбыта, а также планы, имеющие отношение к хозяйственной деятельности Организации;
      2. Досье клиентов (включая их персональные данные) и клиентские списки Организации;
      3. Любой пароль, код доступа, средство или устройство, используемые Организацией для доступа и эксплуатации компьютерных систем, программ или аппаратуры Организации;
      4. Сведения о внутренней структуре Организации;
      5. Сведения о методах управления, используемых Организацией;
      6. Сведения по вопросам управления, кадровым, штатным, правовым вопросам и вопросам региональной политики Организации;
      7. Сведения по экономической, финансовой и бухгалтерской деятельности Организации;
      8. Финансовые отчеты, экономические данные и планы Организации;
      9. Сведения по коммерческой деятельности на внутреннем рынке Организации;
      10. Сведения по вопросам внешнеэкономической деятельности Организации;
      11. Прогнозы продаж, маркетинговая информация, технологии и способы осуществления анализа рынков сбыта, которые применяются Организацией;
      12. Информация, имеющая отношение к работникам Организации (персональные данные), например: телефонные и адресные списки, обзоры эффективности работы, биографии;
      13. Проекты, фотографии, эскизы, чертежи, опытные образцы, рисунки, спецификации, формулы, ноу-хау, технические данные, отчеты, идеи, компьютерные программы, принадлежащие или используемые Организацией;
      14. Сведения и информация, к которым сотрудники Организации получают доступ в рамках использования внутренних информационных сервисов Организации (электронная почта, корпоративный мессенджер, внутренняя база данных и т.д.);
      15. Информация, полученная от третьих лиц, в отношении которой у Организации существуют обязательства по сохранению конфиденциальности.
   2. Режим коммерческой тайны не может быть установлен в отношении сведений, перечисленных в ст. 5 Закона о коммерческой тайне (сведения, содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры; содержащиеся в документах, дающих право на осуществление предпринимательской деятельности; о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов; о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом; о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест; о задолженности работодателей по выплате заработной платы и социальным выплатам; о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений; об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности; о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации; о перечне лиц, имеющих право действовать без доверенности от имени юридического лица; сведения, обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами).
3. **ОХРАНА КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ**
   1. Меры по охране конфиденциальности информации, принимаемые руководителем Организации, включают в себя:
      1. Определение перечня информации, составляющей коммерческую тайну (п. 2.1 Положения);
      2. Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
      3. Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
      4. Регулирование отношений по использованию информации, составляющей коммерческую тайну, сотрудниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
      5. Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения).
4. **ПОРЯДОК ДОПУСКА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**
   1. По всем вопросам деятельности Организации допуск к Конфиденциальной информации имеет руководитель Организации, если иное не определено уставом Организации или иным внутренним документом Организации либо решением вышестоящего над руководителем органа Организации.
   2. По вопросам, относящимся к их компетенции, к Конфиденциальной информации Организации имеют допуск следующие лица:
      1. руководитель Организации;
      2. заместители руководителя Организации;
      3. главный бухгалтер Организации;
      4. Сотрудники, в трудовом договоре которых имеется соответствующее условие о неразглашении конфиденциальной информации;
      5. иные лица, получившие допуск к конфиденциальной информации Организации в соответствии с настоящим Положением.
   3. Допуск оформляется на основании заявления Сотрудника с указанием причины получения определенной информации, а также необходимости копирования с применением технических средств указанной информации.
   4. Заявление рассматривается [руководителем Организации] в течение трех (3) дней. По итогам рассмотрения заявления принимается решение о допуске или отказе в допуске Сотрудника к запрашиваемой им информации.
   5. Решение о допуске или отказе в допуске к конфиденциальной информации оформляется изданием соответствующего распоряжения.
5. **ПОРЯДОК РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ**
   1. Работа с конфиденциальной информацией осуществляется [в специально выделенном помещении, а именно: [указать]] / [в офисе Организации] / [при желании укажите иное].
   2. Если конфиденциальная информация предоставляется Сотрудникам Организации посредством использования определенных сервисов (сайты, приложения, программы и тп.), указанные лица обязаны:
      1. [Использовать исключительно компьютеры Организации];
      2. Соблюдать меры информационной безопасности при работе с сервисами, проявлять бдительность, осторожность и внимательность;
      3. Устанавливать сильные (сложные) пароли с учетом требований и рекомендаций сервисов, в том числе, не использовать пароли длинной менее 8 символов, не использовать стандартные пароли, например «12345678», «qwerty», «password» и т.д., не использовать в качестве пароля дату рождения, не использовать одинаковые пароли в разных сервисах, использовать в пароле символы разных регистров (большие и маленькие буквы), использовать в пароле сочетание букв, цифр, а также специальных символов (например, «!», «@», «$» и др.), если это допустимо сервисом;
      4. Не передавать доступ к сервисам третьим лицам без предварительного получения письменного разрешения с учетом требований Положения;
      5. Если для использования сервиса требуется указание электронной почты, [указывать только корпоративную электронную почту Организации] / [указывать только ту почту, доступ к которой имеется лишь у конкретного лица, получившего доступ к конфиденциальной информации];
      6. Использовать двухфакторную авторизацию там, где это возможно;
      7. Регулярно обновлять операционную систему, программное обеспечение и базу антивируса;
      8. Не использовать устройство, через которое можно получить доступ к конфиденциальной информации, для скачивания файлов с подозрительных сайтов;
      9. Соблюдать политику чистого стола: не оставлять разблокированным рабочее устройство при оставлении рабочего места, не оставлять содержащие конфиденциальную информацию документы на видных местах, не выписывать пароли на бумагу и оставлять на столе и др.;
      10. Соблюдать меры противодействия фишингу: не переходить по ссылкам, получения которых вы не ожидали, уточнять у коллег, контрагентов и др. лиц, действительно ли они присылали письмо, которое вам показалось подозрительным.
      11. В случае потери доступа к сервису (утрата пароля, компьютера или иного устройства, с которого осуществлялось использование сервиса, взлом почты, взлом аккаунта на сервисе и т.д.) незамедлительно сообщить об этом [указать должность] Организации.
   3. Выдача и возврат носителей конфиденциальной информации, а также выдача доступа к сервисам (п. 5.2 Положения) фиксируются в журнале работы с Конфиденциальной информацией.
   4. Сведения о копировании Конфиденциальной информации вносятся в журнал работы с Конфиденциальной информацией.
6. **ХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И КОНТРОЛЬ ЗА ПОРЯДКОМ ДОПУСКА И РАБОТЫ С НЕЙ**
   1. Хранение Конфиденциальной информации осуществляется в [указать физическое место хранения], а также может осуществляться на серверах сервисов (п. 5.2 Положения), если таковые используются Организацией.
   2. Лицо, осуществляющее хранение и выдачу носителей Конфиденциальной информации, а также лицо, осуществляющее выдачу доступа к конфиденциальной информации посредством сервисов (п. 5.2 Положения), назначается приказом руководителя Организации и руководствуется должностной инструкцией.
   3. Контроль за порядком допуска и работы с Конфиденциальной информацией осуществляет [руководитель Организации].
   4. При осуществлении контроля лицо, указанное в п. 6.3 настоящего Положения, проверяет:
      1. ведение журналов учета при работе с Конфиденциальной информацией;
      2. [если помещение установлено в п. 5.1] состояние помещения, предназначенного для работы с Конфиденциальной информацией;
      3. наличие носителей Конфиденциальной информации.
   5. Проверки осуществляются на основании приказа руководителя Организации.
7. **ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ**
   1. Лица, разгласившие Конфиденциальную информацию, а также лица, нарушившие установленный настоящим Положением порядок доступа, работы и хранения Конфиденциальной информации, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.
   2. Сотрудник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются Работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого сотрудника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

\* \* \*

[Генеральный директор] [Наименование юридического лица»]

[ФИО]

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *М.П.*

Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_