ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop®

Юридическая справка для внедрения и использования программного обеспечения Staffcop Enterprise (далее – ПО) с целью мониторинга рабочих процессов

Носит рекомендательный характер

Юридический аспект

Для легального использования DLP-систем необходимо принять ряд организационно-распорядительных мер:

- Разработать локально нормативные акты (далее ЛНА)
- Утвердить ЛНА
- Ознакомить работников с ЛНА

Документальное определение информации ограниченного доступа

Утвердить список информации, относящейся к коммерческой тайне или содержащей сведения конфиденциального характера

Правила работы с информацией ограниченного доступа

Положение о коммерческой тайне, список лиц, имеющих доступ, список паролей и т.д.

Запрет на использование корпоративных ресурсов в личных целях

Внести в ПВРТ внутреннего правого трудового распорядка (далее ПВТР) условия использования корпоративной почты, сети, оборудования работодателя

Ознакомление сотрудников с ЛНА

Чек-лист

1. Наличие ЛНА в организации

- Положение о защите коммерческой тайны с указанием данных, относящихся к коммерческой тайне. Систематизация и документирование информации ограниченного доступа, а также списка допущенных к ней сотрудников.
- NDA с работниками о неразглашении коммерческой тайны (далее КТ).
- Положение о защите персональных данных.
- Согласия работников об обработке, распространения персональных данных (далее ПД).
- Правил внутреннего трудового распорядка (ПВТР).
- Положение/приказ о применении фото/видеонаблюдения и контроля на территории/помещения организации.
- Регламент о выявлении инцидентов и их расследовании.
- Положение об инфобезопасности (минимум - наличие регламента о применении и хранении логина и пароля для входа в CRM систему организации, ЭВМ).

2. Наличие в ПВТР и трудовом договоре (далее ТД) информации (рекомендуемые формулировки)

В ПВТР включить информацию:

- О бережном и экономном использовании материальных ресурсов организации, не допущении использования помещения и имущества, оргтехники, программного обеспечения (далее – ПО), интернета, почты, телефонии и прочие ресурсы в целях, не связанных с рабочим процессом, в том числе для получения личных выгод, прибыли в интересах своего бизнеса.
- Инфраструктура корпоративной телефонии — собственность организации. Организация вправе записывать и контролировать разговоры по служебному телефону и хранить такие записи.
- Организация ограничивает доступ к интернету и предоставляет объем интернет-трафика для выполнения трудовых обязанностей. При этом организация вправе контролировать объем и содержание полученной работниками информации, с целью контроля за надлежащим выполнением ими трудовых обязанностей.
- Организация ограничивает доступ к определенным интернет-ресурсам в случаях, установленных законодательством РФ, или при угрозе безопасности и (или) репутации организации.
- Работник обязан не допускать копирования, распространения, удаления базы данных клиентов, файлов и программ с рабочего компьютера; удаление и (или) изменения служебной (коммерческой) информации на рабочем компьютере; смены паролей доступа к базам данных, файлам, программам и компьютерам организации, а также иных действий, могущих повлечь уничтожение, порчу имущества организации, незаконное получение и разглашение сведений, составляющих коммерческую тайну организации.
- Работник обязан соблюдать конфиденциальность полученной при исполнении трудовых обязанностей информации, связанной с деятельностью организации, а также сведений, составляющих коммерческую и иную охраняемую законом тайн, ставших известными в связи с исполнением работником своих трудовых обязанностей.

В ТД с дистанционным работником:

- Организация предоставляет по акту приема–передачи оборудования и технических средств дистанционному работнику оборудование, программно-технические средства, средства защиты и иные средства для выполнения трудовых обязанностей.
- Дистанционный работник вправе использовать для работы собственное или арендованное оборудование, лицензированные программы для ЭВМ и технические средства с согласия или ведома организации.

Легитимизация - это важно!

Что можно узнать с помощью специализированного программного продукта?

- Факт нарушения (распространения, утечки данных, нарушения дисциплины, регламента производства).
- Определить сотрудника, допустившего нарушение.
- Установить связь между нарушением и действиями сотрудника, которые явились причиной нарушения.

Информация, полученная с помощью ПО, является допустимым доказательством, то есть соответствует нормам нравственности, истинности, а также требованиям закона относительно источника, способа собирания и вовлечения в гражданский процесс

Действующим законодательством установлено:

- Допустимыми доказательствами являются, в том числе сделанные и заверенные лицами, распечатки материалов, размещенных в информационно-телекоммуникационной сети (скриншот).

- Использование аудио- или видеозаписи даже без лица, в отношении которого они производятся, не требуется.

- Все отношения внутри любой организации вытекают из взаимодействия работодателя и работника, использования ими информации и документов.

- В статьях 21, 22 Трудового кодекса РФ (далее - ТК РФ) указаны основные права и обязанности работника и работодателя. Так работник обязан: добросовестно исполнять свои трудовые обязанности, соблюдать правила внутреннего трудового распорядка, соблюдать трудовую дисциплину, выполнять установленные нормы труда, соблюдать требования по охране труда и обеспечению безопасности труда, бережно относиться к имуществу работодателя - то есть выполнять свои трудовые функции в определенное время.

- Работодатель имеет право требовать от работника выполнения должностных обязанностей, в том числе осуществлять контроль за ним (ст. 56 ТК РФ).

- Работодатель обязан предоставить работнику рабочее место, оснащенное рабочим компьютером, доступом в интернет, телефонией и т.д., которые работник использует для выполнения возложенных на него трудовых обязанностей и не имеет права использовать для решения своих личных задач.

- Требование о соблюдении режима рабочего времени, обязательно не только для тех работников, которые работают непосредственно в офисе, но так же распространяются и на работников, которые переведены на удаленный режим работы (дистанционные работники).
- Работодатель в ЛНА должен установить запрет на использование рабочего компьютера, интернет-трафика, телефонии в личных целях. Выполнение этого условия позволяет защитить конфиденциальную информацию организации-работодателя от неразглашения и обеспечить режим коммерческой тайны.
- Работодатель с целью контроля за рабочим процессом также может устанавливать системы фото и видеосъемки в офисе при соблюдении нескольких условий: фото-видео съёмка осуществляется в целях соблюдения законов, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества.
- Установка фото и видео съёмки должна быть закреплена в ЛНА организации - например, в ПВТР.
- Согласно статье 21 ТК РФ работник имеет право на полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем месте.
- Поэтому работник должен быть ознакомлен со всеми ЛНА организации, которые непосредственно связаны с его работой.

Таким образом, программное обеспечение Staffcop Enterprise или иное специализированное программное обеспечение, в том числе видеокамеры, законно могут быть установлены на компьютеры работников при включении соответствующего условия в ЛНА организации.

> Использование работником компьютера (иного оборудования работодателя) для целей, не связанных с рабочим процессом (в том числе в личных), является недобросовестным исполнением работником его трудовой функции.

Поэтому законодательством предоставлено работодателю право устанавливать специальное программное обеспечение (далее - ПО) на рабочие компьютеры, которое позволяет работодателю контролировать выполнение работником трудовых обязанностей и соблюдение им режима рабочего времени.

Мы рекомендуем включить следующие формулировки в ПВТР организации:

«Работники должны бережно и экономно использовать материальные ресурсы организации:

- Не допускается использовать помещения и имущество, оргтехнику, программное обеспечение (далее – ПО), интернет, почту, телефонию и прочие ресурсы в других целях, в том числе для получения личных выгод, прибыли в интересах своего бизнеса.
- Инфраструктура корпоративной телефонии — собственность организации, и предназначена для выполнения работниками своих трудовых обязанностей.
- Организация вправе записывать и контролировать разговоры по служебному телефону и хранить такие записи.
- Организация ограничивает доступ к интернету и предоставляет объем интернет-трафика для выполнения трудовых обязанностей. При этом организация вправе контролировать объем и содержание полученной работниками информации, с целью контроля за надлежащим выполнением ими трудовых обязанностей.
- Организация ограничивает доступ к определенным интернет-ресурсам в случаях, установленных законодательством РФ, или при угрозе безопасности и (или) репутации организации.
- Работник обязан не допускать копирования, распространения, удаления базы данных клиентов, файлов и программ с рабочего компьютера; удаление и (или) изменения служебной (коммерческой) информации на рабочем компьютере; смены паролей доступа к базам данных, файлам, программам и компьютерам организации, а также иных действий, повлекших уничтожение, порчу имущества организации, незаконное получение и разглашение сведений, составляющих коммерческую тайну организации.
- Работник обязан соблюдать конфиденциальность полученной при исполнении трудовых обязанностей информации, связанной с деятельностью организации, а также сведений, составляющих коммерческую и иную охраняемую законом тайны, ставших известными в связи с исполнением работником своих трудовых обязанностей.

Установка видеокамер, специального ПО на личные компьютеры работников, выполняющих работу дистанционно, производится только с согласия такого работника

Рекомендуемые формулировки для включения в форму трудового договора с дистанционным работником:

«Организация предоставляет по акту приема–передачи оборудования и технических средств дистанционному работнику оборудование, программно-технические средства, средства защиты и иные средства для выполнения трудовых обязанностей.
Дистанционный работник вправе использовать для работы собственное или арендованное оборудование, лицензированные программы для ЭВМ и технические средства с согласия или ведома организации».

Необходимо заметить, что использование программного обеспечения Staffcop Enterprise не противоречит Федеральному закону «О персональных данных» № 152-ФЗ.

Обработка персональных данных физического лица допускается в случаях, установленных Законом и если такая обработка персональных данных осуществляется с согласия субъекта персональных данных (п.1 п.1 ст. 6 152- ФЗ), а значит обработка персональных данных работника с помощью программного обеспечения работодателя возможна с момента подписания работником согласия на обработку персональных данных при трудоустройстве.

Резюмируя, советуем до начала использовании ПО Staffcop Enterprise в своей деятельности:

- Подписать согласие на обработку персональных данных со всеми работниками.
- Включить вышеуказанные рекомендуемые формулировки в Правила внутреннего трудового распорядка организации.
- Ознакомить с изменениями, внесенными в Правила внутреннего трудового распорядка или самими Правилами внутреннего трудового распорядка в новой редакции всех работников организации под роспись.
- В трудовой договор с дистанционными работниками включить пункты, содержащие условия использования работником собственного оборудования, с последующей компенсацией работнику в денежной форме.
- Получить согласие от дистанционного работника на установку дополнительного ПО работодателя на личное оборудование дистанционного работника или включить соответствующий пункт в Правила внутреннего трудового распорядка.