Рекомендации по легализации в компании системы мониторинга и DLP

Вопрос 1.	**Какой политики рекомендуется придерживаться работодателю при использовании систем мониторинга в компании?**
Ответ	1. Работодатель является обладателем информации и информационных систем в компании. У него есть право составлять и контролировать нормы по использованию информации. 2. В компании внутренним приказом установлен режим Коммерческой тайны, имеется перечень информации ограниченного доступа и правила работы с ней, инструкция или политика взаимодействия с информацией. Передача такой информации при помощи личных средств связи (например, личной электронной почты) запрещена законом. 3. Работодатель не берет на себя обязательства сотового оператора, телеграфа или почты, предоставленные средства связи являются не услугами, а техническими средствами и инструментами для работы. 4. Сотрудники письменно уведомлены о возможном применении систем мониторинга в компании с целью контроля исполнения норм трудового распорядка и работы со служебной информацией. 5. Сотрудники уведомлены о запрете на использование, хранение личной информации на корпоративных устройствах и ресурсах. 6. Предполагается, что на корпоративных ресурсах нет личной информации сотрудников, а у работодателя нет намерений раскрыть чью-то личную тайну. 7. Личная информация подлежит удалению в случае ее обнаружения на корпоративных ресурсах компании. Сотрудник несет ответственность за несоблюдение трудовой дисциплины. 8. Личные данные сотрудника при принятии решения работодателем использованы не будут в случае обнаружения таковых. 9. У работодателя нет умысла нарушить тайну переписки сотрудника, поэтому личные средства хранения информации, такие как электронная почта или социальные сети, не взламываются и не проверяются. 10. В целях контроля информации ограниченного доступа и соблюдения правил внутреннего трудового распорядка, работодатель использует данные, которые собраны с рабочего места сотрудника.
Вопрос 2.	**Что рекомендуется сделать, чтобы повысить правовую значимость системы мониторинга и иметь возможность апеллировать к ней в суде?**
Ответ	В сфере информационной безопасности рекомендуется: 1. Внутренним приказом установить в компании режим Коммерческой тайны. 2. Документировать правила обработки информации ограниченного доступа (конфиденциальная, служебная информация, коммерческая тайна и другое). 3. Важным моментом является систематизация и документирование информации ограниченного доступа, а также списка допущенных к ней сотрудников.

4. Во внутренних правилах необходимо запретить разглашение информации ограниченного доступа, определить условия ее защиты, ответственность за хранение и разглашение.
5. Запретить хранение личных данных на корпоративных ресурсах и устройствах, запретить использование в неслужебных целях корпоративное оборудование, ПК, ноутбуки, оргтехнику.
6. Письменно уведомлять сотрудников о возможном мониторинге за их рабочим местом.
7. Своевременно знакомить работников с требованиями информационной безопасности.
8. Отношения регулировать через трудовой договор с сотрудниками и договор с подрядчиком.
9. На всех материальных носителях, содержащих Коммерческую тайну, наносить гриф конфиденциальности.

Вопрос 3.	**Какие положения рекомендуется включить во внутренние документы?**
Ответ	При внедрении в организации средств мониторинга и DLP-систем, в нормативной базе работодателя рекомендуется: - прописать правила и порядок использования средств электронной коммуникации (в том числе запретить использование личной почты в служебных целях, несанкционированный вынос информации, оборудования); - запретить использование сотрудниками в неслужебных целях оборудования и программного обеспечения работодателя; - раскрыть право работодателя на контроль и мониторинг рабочего места сотрудников, добровольное согласие на то работника. Содержание внутренних документов зависит от специфики компании работодателя. Если перечисленные выше правила не закреплены во внутренней документации, то их можно внести в Правила внутреннего трудового распорядка, можно в Должностную инструкцию или в Трудовой договор (Дополнительное соглашение к договору). Текст может иметь следующий вид: «Работнику запрещается: - Допускать третьих лиц к конфиденциальной информации. - Размещать в сети Интернет конфиденциальную информацию. - Вести деловую переписку с использованием личной электронной почты. - Хранить сведения, составляющие личную и семейную тайну на рабочем месте и корпоративных устройствах.» «Работник уведомлен и выражает свое согласие на то, что: - Работодатель имеет право применения средств контроля за соблюдением Работником правил внутреннего трудового распорядка. - В качестве средств контроля Работодатель имеет право использовать специальное программное обеспечение и системы наблюдения за рабочим местом сотрудника». Также проинформировать сотрудников о мониторинге рабочих мест можно через официальный приказ и расписку об ознакомлении.