ЭЛЕКТРОННАЯ СВЯЗЬ И ЭЛЕКТРОННЫЕ ДАННЫЕ ОБ ИНСПЕКЦИИ ПРАВИЛА

KVKK_Y4 ВЕРСИЯ 1.00

1. ЦЕЛЬ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Целью настоящего Положения является определение процедур и принципов, касающихся условий и сроков мониторинга электронных коммуникаций Компании, и положения настоящего Положения распространяются на персонал и третьих лиц, уполномоченных получать доступ к средствам электронной связи Компании и/или использовать их.

2. Мониторинг электронных коммуникаций

2.1. Для целей настоящего Регламента под электронной коммуникацией обычно понимаются все виды электронных сообщений, включая телефонные звонки, факсимильные сообщения, электронную почту, мгновенные сообщения, SMS или другие короткие сообщения, твиты, вики-страницы, блоги и веб-контент, публикуемый на платформах обмена сообщениями. В силу специфики своей деятельности Компания не несет ответственности или обязанности по общему мониторингу содержания электронных сообщений своего персонала или посетителей. Кроме того, Компания не проводит регулярной общей проверки электронных сообщений путем случайной выборки или вмешательства человека. Однако автоматизированная компьютерная проверка электронной почты осуществляется в ограниченном объеме для предотвращения нежелательных массовых рассылок электронной почты (обычно называемых «спамом») и потенциально вредоносного содержимого сообщений (компьютерные вирусы, попытки финансового мошенничества и т. д.).

2.2.5.4. Все пользователи подтверждают, что, используя электронные системы связи, предоставляемые Компанией, Компания не дает никаких гарантий относительно конфиденциальности каких-либо сообщений или данных, хранящихся в указанных системах или передаваемых через них; что Компания сохраняет за собой права, указанные в настоящем документе; и что использование указанных систем ограничено целями, одобренными Компанией, и что пользователи были уведомлены об этом. Использование электронных систем связи Компании в связи с деятельностью Компании и для личного использования, не являющегося необходимым, не является правом, а привилегией, предоставляемой ее сотрудникам и уполномоченным третьим лицам.

Таким образом, Компания может в любое время и без предварительного уведомления полностью или частично заблокировать доступ ко всем или части своих электронных коммуникационных и ИТ-систем (для всех или некоторых пользователей). Пользователи электронных коммуникационных и компьютерных систем Компании обязаны соблюдать Положение Компании о порядке и принципах использования информационно-коммуникационных технологий и Раздел 11.9 «Условия допустимого использования ИТ-ресурсов (Политика допустимого использования)» Политики информационной безопасности, и, используя указанные системы, они подтверждают, что приняли и будут соблюдать Политику допустимого использования, что они были уведомлены об этом и что они дали свое согласие на внедрение Компанией Политики допустимого использования. Пользователи также соглашаются соблюдать соответствующее законодательство и воздерживаться от любых действий, которые могли бы обязать Компанию. Компания может в любое время и без предварительного уведомления изменять Положение о порядке и принципах надлежащего использования Интернета и средств электронной связи, а также другие условия, касающиеся использования компьютерных систем.

Мы оставляем за собой право вносить изменения и предпринимать любые действия, необходимые или целесообразные в соответствии с действующим законодательством.

2.3. В соответствии со статьей 6 Закона № 5651 «О регулировании публикаций в Интернете и борьбе с преступлениями, совершаемыми посредством таких публикаций», озаглавленной «Обязанности поставщика доступа», Компания обязана принимать необходимые меры для хранения информации о трафике электронных коммуникаций, полученной или отправленной Компанией, в целях, указанных в законе, и для обеспечения точности, целостности и конфиденциальности этой информации. Эти меры включают, помимо прочего, мониторинг использования информации в преступных или несанкционированных целях, проведение аудитов и мероприятий по защите системы от таких угроз, как вирусы, хакерские атаки и атаки типа «отказ в обслуживании», а также обеспечение соответствия ИТ-операций политике и директивам Компании.

2.4. Мониторинг электронных коммуникаций будет осуществляться преимущественно с согласия соответствующего лица. Однако Компания оставляет за собой право проводить мониторинг по собственной инициативе для достижения своих законных целей в следующих случаях:

2.4.1. Ведение учета сделок и иных сообщений, если необходимо или желательно знать определенные элементы коммуникации между заинтересованными сторонами для обеспечения безопасности финансово-экономической деятельности и сделок;

2.4.2. Подтверждать соответствие нормативным актам и правилам, касающимся Компании, например, проверять, соблюдаются ли административные положения Компании, а также внутренние руководящие принципы и кодексы поведения;

2.4.3. Определять или демонстрировать стандарты, которым должны соответствовать лица, использующие электронные информационные системы Компании в таких целях, как контроль качества или обучение персонала;

2.4.4. Мониторинг или запись с целью предотвращения или выявления преступных деяний, например, коррупции, неправомерного использования компьютерных систем или другой незаконной деятельности.

2.4.5. Для предотвращения или выявления несанкционированного использования электронных информационных и коммуникационных систем, например, для предотвращения нарушений сотрудниками правил Компании, упомянутых в Разделе 11: «Условия использования ИТ-ресурсов (Политика допустимого использования)» Политики информационной безопасности;

2.4.6. Для обеспечения эффективной работы системы путем обнаружения и удаления вирусов, контроля и предотвращения других угроз системе, таких как взлом или атаки типа «отказ в обслуживании»; а также путем создания сетевых потоков и журналов электронной почты;

2.5. Лица, использующие электронные системы связи Компании, должны знать, что администраторы информационных и коммуникационных технологий и сетей периодически отслеживают передачи или информацию о транзакциях для обеспечения надлежащего функционирования ИТ-сервисов Компании. В таких случаях соответствующий персонал может непреднамеренно получить доступ к электронной информации.

Они могут быть осведомлены о содержании сообщения. Если иное не указано в настоящем Положении или соответствующем законодательстве, указанным должностным лицам запрещается сознательно просматривать содержание информации о транзакциях сотрудников Компании или иным образом использовать увиденное, услышанное или прочитанное ими. Однако, если будет обнаружено нарушение политики Компании и административных правил или правовых положений, об этом необходимо сообщить высшему руководству Компании.

3. АНАЛИЗ ЭЛЕКТРОННЫХ ДАННЫХ

3.1. Компания может периодически проверять корпоративную электронную почту, хранящуюся на сетевых или независимых устройствах хранения данных, документы и файлы, расположенные на локальных, основных или групповых дисках, а также данные, относящиеся к записям доступа к системам или зданиям Компании. Кроме того, считается, что сотрудники и посетители, подключающиеся к сети Компании со своих индивидуальных устройств, дали согласие на мониторинг своих данных в целях, ограниченных теми, которые указаны в разделе 6 Политики информационной безопасности Компании, озаглавленном «Мониторинг электронных коммуникаций». Эти проверки ограничиваются обеспечением безопасности данных и будут проводиться в соответствии с принципами, изложенными в Законе № 6698 о защите персональных данных.

3.2. В обычных условиях Компания получит согласие пользователя перед проведением любого анализа данных, хранящихся у физических лиц или относящихся к ним, таких как учетные записи электронной почты, основные или локальные драйверы, а также записи журналов доступа. Однако анализ будет проводиться даже без согласия пользователя в следующих случаях:

3.2.1. Там, где это предусмотрено законом;

3.2.2. Если имеются достоверные доказательства, выходящие за рамки простых сплетен или слухов, и есть серьезные подозрения в нарушении правовых положений или политики Компании;

3.2.3. В исключительных обстоятельствах и чрезвычайных ситуациях, когда бездействие может привести к серьезному физическому вреду, значительному ущербу имуществу, утрате важных доказательств нарушения закона или политики и правил Компании, или к значительным финансовым обязательствам перед Компанией или ее сотрудниками и/или директорами;

3.2.4. Бездействие может повлиять на административное или финансовое функционирование Компании.

если существует вероятность того, что их способность выполнять свои обязанности будет серьезно ограничена.

3.3. Если соответствующий пользователь находится вне зданий и сооружений Компании, и проверка данных, хранящихся у пользователя или относящихся к нему, необходима по коммерческим причинам, необходимо предварительно получить согласие соответствующего пользователя. Если связаться с пользователем невозможно, руководитель соответствующего отдела и генеральный директор могут предоставить письменное разрешение на проведение проверки компьютера или других устройств, предоставленных пользователю для ведения дел Компании. В этом случае необходимо получить соответствующее согласи

Меры и причины, побудившие к проведению проверок, будут зафиксированы в отчете.

3.4. Если возникает необходимость в просмотре данных, хранящихся у пользователя или относящихся к физическим лицам, как указано в пункте 3.2 выше, без получения согласия субъекта данных, применяются следующие правила:

3.4.1. Чрезвычайные ситуации: Могут быть рассмотрены минимальные требования чрезвычайной ситуации, и минимальные меры, необходимые для ее устранения, могут быть приняты немедленно без разрешения; однако, как только чрезвычайная ситуация минует, необходимо незамедлительно получить соответствующее разрешение и зафиксировать ситуацию в соответствии с пунктом 3.3;

3.4.2. Во всех остальных случаях никакие действия не будут предприниматься без письменного разрешения соответствующего руководителя отдела и генерального директора.

3.4.3. Зашифрованные данные: Если в ходе проверки системы обнаружены зашифрованные данные, ключ расшифровки должен быть предоставлен по запросу.

3.4.4. Данные, созданные сотрудниками, которые больше не работают в нашей Компании, или относящиеся к ним, принадлежат Компании и подлежат уничтожению в соответствии с положениями законодательства о сроках уничтожения данных. Для ознакомления с такой информацией не требуется получать разрешение уволенного сотрудника. Разрешение на просмотр информации должно быть получено в соответствии с процедурой, указанной в пункте 3.3 выше.

3.5. После получения разрешения данные в системах Компании будут обрабатываться следующим образом:
будет обсуждаться:

3.5.1. Материалы, относящиеся к деятельности компании, будут оцениваться в соответствии с обычной деловой практикой. Они будут сохранены или удалены по мере необходимости.

3.5.2. Персональные данные не будут проверяться без законных оснований.

3.5.3. Сотрудники компании обязаны удалить свои персональные данные, содержащиеся в электронных документах и электронных письмах, до прекращения трудовых отношений.

3.6. Конфиденциальность: Все проверки, проводимые в соответствии с настоящим Положением, будут осуществляться с должным учетом права на неприкосновенность частной жизни. Материалы, касающиеся частной жизни отдельных лиц, будут подвергаться минимальной проверке, необходимой для целей проверки. Любая обнаруженная конфиденциальная информация, не имеющая отношения к цели проверки, не будет разглашена третьим лицам и останется конфиденциальной. Однако, если в ходе проверки будут обнаружены какие-либо материалы, являющиеся незаконными или противоречащие политике Компании, об этом будет немедленно сообщено Генеральному директору, и будут приняты меры в соответствии с его указаниями.