ПРИНЯТИЕ ИНТЕРНЕТА И ИНСТРУМЕНТОВ ЭЛЕКТРОННОЙ КОММУНИКАЦИИ И ВОЗМОЖНОЕ ИСПОЛЬЗОВАНИЕ ПОЛИТИКА В ОТНОШЕНИИ ПРОЦЕДУР И ПРИНЦИПОВ

KVKK_P9 ВЕРСИЯ 1.00

Компания KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED

ИНТЕРНЕТ И ИНСТРУМЕНТЫ ЭЛЕКТРОННОЙ КОММУНИКАЦИИ ПРОЦЕДУРЫ ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ

ПОЛИТИКА В ОТНОШЕНИИ ПРИНЦИПОВ

1. ВВЕДЕНИЕ

Компания Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi, являясь частным юридическим лицом, обязана обеспечивать надлежащее использование всех выделенных ей ресурсов и предотвращать их нецелевое или неправомерное использование, не соответствующее их назначению. Эта ответственность включает в себя использование таких услуг, как электронная почта (e-mail) и доступ в Интернет.

2. ЦЕЛЬ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Цель данной политики — определить процедуры и принципы, которые сотрудники нашей компании должны соблюдать при использовании электронных средств связи, таких как интернет и электронная почта. Политика состоит из трех частей:

- Правила использования интернета •
  Правила использования электронной почты
- Электронная связь между сотрудниками

Настоящая Политика должна рассматриваться в совокупности со следующими нормативными документами:

- Дисциплинарные правила компании
- Политика защиты и обработки данных • Политика
  информационной безопасности

В целях настоящей Политики все формы электронной связи, включая электронную почту, веб-почту, мгновенные сообщения и веб-форумы, должны толковаться как охватывающие все формы электронной связи. Если доступ к интернету и электронной почте, предоставляемый Компанией, осуществляется через беспроводную сеть внутри здания Компании или через доступ с рабочего стола извне, считается, что соответствующая сторона приняла положения настоящей Инструкции.

3. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА

3.1. Цели предоставления услуг и обязанности пользователей:

Интернет-услуги изначально и в первую очередь предоставляются для осуществления деловой деятельности компании. Индивидуальное использование допустимо при условии разумного, внимательного и ответственного подхода, особенно когда сотрудники используют интернет в личных целях.

3.2. Мониторинг использования:

3.2.1. Сотрудники, использующие корпоративную интернет-сеть, не имеют разумных оснований ожидать неприкосновенности частной жизни или сохранения конфиденциальности. Компания использует защищенные сетевые сайты и ссылки для записи поисковых запросов в интернете и предотвращения несанкционированного доступа к ним со стороны сотрудников.

Система использует следующие сервисы . Управление системой осуществляется ИТ-менеджером, а мониторинг проводят руководители отделов и Совет директоров. Межсетевой экран периодически тестируется для выявления любых потенциальных недостатков или уязвимостей в системе.

3.2.2. Программное обеспечение для мониторинга. Программное обеспечение отслеживает использование интернет-сети компании, а ИТ-отдел и руководители отделов контролируют и проверяют журналы сети, чтобы обеспечить использование в соответствии с политикой компании. Это включает в себя удаленное сканирование мониторов компьютеров, проверку файлов и электронной почты, а также анализ посещенных веб-сайтов. Программное обеспечение записывает все посещенные веб-сайты, а также соответствующее имя пользователя и дату/время посещения, и генерирует регулярные отчеты для целей мониторинга. О подозрительных или неправомерных посещениях и веб-сайтах будет автоматически сообщаться, и будут инициированы стандартные дисциплинарные процедуры. Получая доступ к интернет-сети компании, пользователи считаются давшими согласие на описанные выше действия по мониторингу и контролю доступа в интернет.

3.3. Персональная подписка и использование в развлекательных целях:

Сотрудникам запрещается оформлять подписки на услуги интернет-провайдеров и/или онлайн-сервисы внутри компании и использовать их на компьютерном оборудовании компании без письменного согласования с ИТ-менеджером. Сотрудникам запрещается использовать интернет-сервис в ненадлежащих развлекательных целях, таких как компьютерные игры или азартные игры.

3.4. Действия, которые могут нанести ущерб репутации компании:

Сотрудникам запрещается использовать интернет способом, противоречащим интересам Компании, причиняющим вред Компании и ее партнерам или наносящим ущерб ее корпоративной репутации. Например, подписка на веб-сайты, содержащие запрещенные или незаконные материалы, или использование или загрузка защищенного авторским правом контента от третьих лиц без явного разрешения правообладателя.

3.5. Установка программного обеспечения (загрузка):

Для минимизации вирусных рисков и предотвращения распространения нелицензионного программного обеспечения в сети установка программного обеспечения с использованием корпоративной сети запрещена. Этот запрет также распространяется на игры и заставки. Если для целей обучения персонала необходимо исключение из этого запрета, пожалуйста, свяжитесь с ИТ-отделом.

3.6. Незаконное использование:

Сотрудникам запрещается сознательно использовать интернет для действий, нарушающих турецкое законодательство. Нашим сотрудникам запрещается использовать интернет для поиска, скачивания, доступа или иного поиска материалов, которые могут оскорбить или дискриминировать других сотрудников по признаку пола, расы, религиозных убеждений, сексуальной ориентации, инвалидности или по другим причинам.

3.7. Интернет-магазин:

Сотрудникам может быть разрешено совершать онлайн-покупки в течение продленного рабочего времени. Однако важно помнить, что не следует устанавливать программное обеспечение продавца на свой компьютер или другие устройства. Хотя предоставляемая сеть не имеет более низких стандартов безопасности, чем сети, используемые для частных домов, наша компания не несет ответственности за безопасность финансовых транзакций. Покупки ни в коем случае не должны включать товары, которые являются «непристойными, порнографическими или вторгаются в частную жизнь», а также товары, относящиеся к категории запрещенных действий.

3.8. Безопасность:

Как сотрудники, ответственные за доступ к сети и ее безопасность, крайне важно не сообщать никому свои имя пользователя и пароль. В этом контексте компьютеры следует блокировать, когда вы не находитесь за компьютером, нажав Ctrl-Alt-L или Ctrl-Alt-Del. В случае утери или кражи личных устройств, используемых для доступа к корпоративной электронной почте или данным, необходимо немедленно уведомить ИТ-отдел. Наши сотрудники также должны быть ознакомлены с Политикой информационной безопасности, которая содержит подробную информацию о защите паролей и безопасности.

3.9. Запрещенные виды деятельности:

К запрещенным в интернете видам деятельности относятся следующие инструменты:
Это включает в себя мониторинг, хранение, распространение или любое другое использование продукта.

• Незаконная деятельность (включая все формы нарушения авторских прав) • Угрожающее, оскорбительное, преследующее или дискриминационное поведение
• Виды клеветы и клеветнические намерения и действия • Непристойные, провокационные или личные сообщения, изображения, вызывающие возмущение, или порнографические материалы • Все, что может причинить вред нашей Компании без предварительного разрешения деятельность

• Рассылка писем по электронной почте • Индивидуальная или коммерческая деятельность с целью получения прибыли • Злонамеренные и вредоносные действия • Ненадлежащее использование в политических, религиозных или развлекательных целях.

3.10. Обязанность защищать:

Любой сотрудник, случайно получивший доступ к изображениям, содержащим материалы с изображением насилия над детьми, во время использования корпоративной сети, обязан немедленно сообщить о местонахождении изображений в ИТ-отдел и не должен делать копии этих изображений или распространять их кому-либо.

3.11. Вопросы безопасности и доступа:

3.11.1. Компания приняла меры для защиты себя, своих компьютерных систем, веб-сайтов и сотрудников от текущих и потенциальных внешних и внутренних угроз безопасности. Эти меры безопасности включают, помимо прочего, следующее: межсетевые экраны и прокси-серверы, используемые для блокировки входящего/исходящего интернет-трафика; антивирусное программное обеспечение; программное обеспечение для контроля доступа (блокирующее доступ к определенным веб-сайтам); меры по предотвращению установки программного обеспечения; и программное обеспечение, ограничивающее потенциально вредоносные скрипты и элементы.

3.11.2. Компания получает услуги фильтрации от своего интернет-сервера. Хотя доступ в интернет для сотрудников, использующих ее сеть, дополнительно не блокируется Компанией, она может блокировать доступ к сайтам, содержащим или предположительно содержащим незаконный, порнографический или иной контент, вызывающий беспокойство (например, сообщения сексуального характера, веб-чаты, преступная деятельность, наркотики, алкоголь и табак, азартные игры, сайты знакомств и дружбы, новости Usenet, насилие и оружие и т. д.).

3.11.3. Пользователи Интернета должны знать, что многие веб-сайты иногда тайно записывают данные об использовании сайта, и что доступ в Интернет и активность оставляют записи на их ПК.

3.11.4. Компания оставляет за собой право прерывать доступ в Интернет без предварительного уведомления, если она подозревает нарушение безопасности, требующее немедленных действий, или если она оценивает, что сеть и/или компьютерные системы Компании находятся под угрозой.

4. ПОЛИТИКА И ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

4.1. Цель настоящей политики — обеспечить надлежащее использование систем электронной почты.

Каждый сотрудник, имеющий доступ к почтовой службе, обязан соблюдать положения настоящей Политики и обеспечивать ответственное, эффективное и только в утвержденных целях использование почтовой системы. Цель настоящей политики — предоставить информацию, которая послужит руководством для сотрудников, особенно в отношении внутренней коммуникации компании по электронной почте. Например, личное использование корпоративной почтовой системы запрещено.

4.2. Статус электронной переписки:

Наши сотрудники всегда должны помнить, что электронная переписка — это документ, который может быть раскрыт в судебном порядке при общении по электронной почте. Все электронные сообщения, отправленные или полученные в корпоративной сети электронной почты, являются собственностью компании, и пользователи не должны рассчитывать на конфиденциальность личных данных при использовании системы электронной почты. ИТ-отдел имеет право отслеживать электронные сообщения и сетевые журналы для обеспечения соблюдения политики компании. Считается, что все пользователи дали согласие на такой мониторинг и проверку электронной почты.

4.3. Личная электронная почта:

Пользователи системы электронной почты могут отправлять и получать внутренние и внешние личные сообщения. Однако такое использование не должно мешать работе пользователя или работе другого пользователя, а также препятствовать выполнению пользователем своих обязанностей. Следует избегать чрезмерного использования электронной почты в личных целях. Система электронной почты не может использоваться для частной деловой деятельности или для разглашения, распространения или иного распространения конфиденциальной информации, принадлежащей Компании.

4.4. Содержание:

Все электронные письма, как явные, так и неявные, должны быть свободны от упоминаний сексуального, расового или религиозного характера, преступлений или домогательств и должны быть написаны с использованием только языка, приемлемого для профессионального общения на рабочем месте.

4.5. Конфиденциальность:

Конфиденциальность электронных сообщений не гарантируется. Любое отправленное или полученное сообщение может быть доступно коллегам, не являющимся получателем, как случайно (например, из-за оставленной открытой сессии компьютера), так и преднамеренно (например, электронное письмо может потребоваться открыть для диагностики проблем с подключением). Поэтому сообщения нельзя считать частными или конфиденциальными. Личные сообщения следует писать с учетом возможности просмотра их содержимого третьими лицами. Что касается внешних электронных писем, они по своей природе небезопасны и могут быть перехвачены и прочитаны третьими лицами без нашего ведома. Сообщения, требующие особого уровня конфиденциальности или деликатности, следует отправлять альтернативными способами и с использованием методов, указанных в Политике информационной безопасности и безопасности передачи данных.

4.6. Вложения файлов:

Чтобы предотвратить копирование неприемлемых материалов в корпоративную сеть и снизить риск заражения вирусами, файлы, прикрепленные к электронным письмам (изображения, текст или содержимое электронных таблиц), можно загружать только в том случае, если они поступают из надежных источников – то есть от контактов, личности которых вам известны, – и не содержат неприемлемого контента. Прикрепленные к электронным письмам исполняемые файлы программ открывать не следует. Вместо этого такие сообщения следует переслать ИТ-менеджеру для консультации. К исполняемым файлам относятся файлы с расширениями: .EXE, .COM, VBS, .SCR, game.exe и screen.scr.

4.7. Письма-цепочки/Шутки:

Рассылка писем по цепочке и юмористическая переписка представляют собой нецелевое использование времени и ресурсов сотрудников компании и могут непреднамеренно оскорбить получателя. Такие сообщения не следует пересылать другим пользователям, и их следует удалять из сети после того, как они попадут в почтовый ящик.

4.8. Ложные предупреждения о вирусах:

Сообщения от сторонних лиц, содержащие предупреждения о вирусах, не следует пересылать другим пользователям. На практике большинство таких сообщений необоснованны. Однако во всех случаях их следует удалять из папки «Входящие» после обращения в службу ИТ-поддержки и получения их рекомендаций.

4.9. Использование внешних систем электронной почты для корпоративных транзакций:

Вся электронная переписка, касающаяся деловых вопросов и транзакций компании, должна осуществляться через корпоративную почтовую сеть. Использование частных почтовых систем и учетных записей (например, AOL, Hotmail, почтовых сервисов, предоставляемых интернет-провайдерами, и других почтовых сервисов, не упомянутых здесь) для деловых целей компании запрещено. Сотрудникам, которым необходимо получить доступ к корпоративной сети вне здания компании, следует обратиться в службу поддержки ID за консультацией по вопросам удаленной работы.

4.10. Рекомендации по отправке электронных писем:

4.10.1. Идентификация получателей электронных писем:

a) Тщательно проверяйте: чтобы избежать распространенных ошибок при отправке электронных писем, таких как неправильное использование значков «Ответить всем» и «Ответить», адреса получателей следует тщательно проверять перед отправкой писем.

b) Основной получатель: Помимо указания основного получателя в адресной строке заголовка электронного письма, заголовок сообщения должен быть «Сообщение для xxxx» или «Уважаемый/Г-н/Г-жа xxxx», чтобы четко указать, кто является получателем и кто должен ответить. Копии (CC) следует указывать только для информационных целей. При отправке электронного письма необходимо указывать копию (CC).

В поле «Копия» вы указываете человека, которого хотите проинформировать по данному вопросу, даже если он не является непосредственным получателем письма. Если вы добавите кого-то в копию, это будет видно всем, кто получит письмо. Другими словами, добавив кого-то в копию, вы подразумеваете, что этот человек будет в курсе письма.

c) Списки получателей (CC): Как и при составлении письма или сообщения, каждый пользователь должен тщательно выбирать получателя и список получателей для копирования. В частности, следует избегать использования нескольких списков получателей (CC) в одном письме. Необходимо тщательно проанализировать, есть ли реальная и эффективная цель для копирования информации или запроса информации от каждого человека, чья информация копируется. Списки получателей (CC) не следует использовать для писем, отправляемых группам клиентов; такие сообщения следует отправлять через портал. Особое внимание следует уделять тому, чтобы не использовать списки адресов электронной почты в полях «Кому» или «Копия», чтобы уважать конфиденциальность получателей.

d) Списки скрытой копии (BCC): «BCC» означает «закрытая копия». Адрес электронной почты, указанный в этом поле, получит нужное сообщение. Получатели в полях «Кому» и «Копия» не видят адреса электронной почты, указанные в этом поле. Эту информацию могут видеть только отправитель и получатель, чей адрес электронной почты указан в этом поле. Однако те, чьи имена указаны в поле «BCC», могут видеть, кто является получателями в полях «Кому» и «Копия».
Хотя использование скрытой копии (BCC) может быть уместно в электронных письмах, отправляемых третьим лицам, сокрытие конфиденциальной информации от одного или нескольких участников в профессиональной переписке может быть плохой идеей, поскольку электронные письма могут быть пересланы позже, потенциально раскрывая информацию, которая должна оставаться конфиденциальной. При таком способе обмена сообщениями, которые некоторые считают личными, могут возникнуть проблемы с доверием, поэтому использование скрытой копии, как правило, следует избегать среди коллег.

e) Массовая рассылка электронных писем: Массовая рассылка электронных писем должна использоваться только в служебных целях компании. Она ни при каких обстоятельствах не может использоваться для отправки индивидуальных сообщений. Кроме того, недопустимо рекламировать или рекомендовать товары и услуги третьих лиц.

f) Отправка вложений в виде документов/таблиц: Электронная почта может использоваться для рассылки напоминаний или других вложений в виде документов. Однако файлы и вложения размером более 10 МБ не следует отправлять по электронной почте. Специалисты ИТ-поддержки могут предоставить рекомендации по отправке больших файлов с использованием таких методов, как общее хранилище.

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ:

Любая переписка, содержащая персональные данные, будет регулироваться действующим законодательством о защите данных. Политика нашей компании по обработке и защите персональных данных и...

Политика информационной безопасности содержит подробную информацию о том, как будут обеспечиваться безопасность персональных данных, и каждый сотрудник должен быть с ней ознакомлен.