ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПОЛИТИКА

KVKK_P5 ВЕРСИЯ 1.00

Компания KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Цель:

Информация играет основополагающую роль в обеспечении всех видов деятельности компании Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi. Надлежащая защита всей информации, обрабатываемой нашей компанией, имеет важное значение для успеха нашей экономической и административной деятельности. Достижение этой цели планируется путем решения трех основных задач информационной безопасности: конфиденциальность данных, целостность данных и доступность/наличие данных, которые являются важнейшими элементами защиты информации компании.

Цели настоящей Политики заключаются в следующем:

1.1. Информационные ресурсы компании надлежащим образом защищены от потери, неправомерного использования и утечек. обеспечить определенный уровень защиты;

1.2. Все пользователи соглашаются с настоящей Политикой и другими связанными с ней нормативными документами и кодексами поведения. и обеспечить их информированность о руководящих принципах;

1.3. Все пользователи подчиняются применимому турецкому законодательству и своим обязанностям в этом контексте. чтобы убедиться, что они осознают свои обязанности;

1.4. Повышать осведомленность сотрудников и других заинтересованных сторон о необходимости внедрения соответствующих мер безопасности на всей территории Компании в рамках цели эффективного функционирования и поддержки информационной безопасности;

1.5. Обеспечить осведомленность всех пользователей об их обязанностях в отношении конфиденциальности, целостности и доступности обрабатываемых ими данных;

Настоящая Политика должна рассматриваться совместно с Политикой обработки и защиты персональных данных компании Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi и соответствующими принципами ее реализации, которые содержат подробную информацию о защите персональных данных.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ:

Данная политика охватывает защиту электронных информационных активов, полученных в результате коммерческой деятельности, осуществляемой в рамках Компании, а также связанных с ней логистических, складских, бухгалтерских, финансовых, контрольно-качественных, закупочных, кадровых, юридических, торговых, маркетинговых, внутренних аудиторских и информационных процессов, а также процессы обеспечения информационной безопасности, используемые компанией Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi для обеспечения обработки, хранения, защиты, конфиденциальности и целостности персональных данных, хранящихся в Компании, в соответствии с законодательством.

2.1. Все сотрудники Компании и все другие соответствующие третьи стороны, включая гостей, уполномоченных получать доступ к информации, контролируемой Компанией или от ее имени, обязаны соблюдать Политику информационной безопасности и соответствующие принципы ее реализации, изложенные в настоящем документе. Положения настоящей Политики охватывают процессы, посредством которых вышеупомянутые стороны получают доступ и используют все данные и программное обеспечение, принадлежащие Компании или лицензированные для использования Компанией, путем прямого или косвенного подключения к сетям, предоставляемым Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi, с использованием устройств, принадлежащих/арендованных и/или предоставленных Компанией, а также всех других внешних инструментов и систем, как внутри Компании, так и через внешние системы.

2.2. Настоящая Политика распространяется на все данные, хранящиеся в Компании, будь то электронные или физические, включая данные, указанные ниже:

- Электронные данные, хранящиеся и обрабатываемые настольными и портативными компьютерами и другими устройствами, а также устройствами хранения данных;
- Передача данных по сетевым средам;
- Информация, отправленная с использованием факса или аналогичных методов передачи;
- Все бумажные документы; • Визуальные и фотоматериалы, включая микрофиши, слайды и записи с камер видеонаблюдения; аудиоданные, относящиеся к голосовым сообщениям и записанным разговорам, в том числе к общению лицом к лицу;

2.3. Данные компании, как правило, можно разделить на персональные и неперсональные данные:

- Обработка персональных данных осуществляется в соответствии с Политикой компании по обработке и защите персональных данных и подлежит защите на самом высоком уровне;
- К неперсональным данным относятся следующие типы данных:
  - я. Особые категории данных компании, включая коммерчески конфиденциальные данные планирования, данные исследований и анализа, данные, защищенные соглашениями о конфиденциальности, а также данные, которые по закону обозначены как привилегированные или конфиденциальны Данные, относящиеся к этой категории, подлежат высокому уровню защиты.
  - ii. Данные компании, ставшие общедоступными после публикации на корпоративном веб-сайте компании, или другие данные компании, которые могут быть обнародованы в соответствии с законодательными нормами, такими как Закон о свободе информации. Крайне важно, чтобы содержание данных в этой категории было точным и актуальным, а также защищено от потери и несанкционированного доступа.

2.4. Положения настоящей Политики применяются ко всем этапам жизненного цикла данных, включая сбор, хранение, обработку и уничтожение данных.

2.5. Хотя использование социальных сетей нашими сотрудниками является бесплатным и не регулируется напрямую Компанией, наша Компания ожидает от своих сотрудников соблюдения положений настоящей Политики и воздержания от действий, которые могут нанести ущерб корпоративной репутации Компании.

Это требует от пользователей воздерживаться от подобного поведения. Для получения подробной информации по этому вопросу, пожалуйста, ознакомьтесь с Политикой использования социальных сетей.

3. ОБЯЗАННОСТИ И ПОЛНОМОЧИЯ:

Обязанности и полномочия сотрудников определены в их должностных инструкциях, наряду с их квалификацией и компетенциями. Обязанности соответствующих подразделений и персонала по поддержанию и совершенствованию деятельности в области информационной безопасности следующие:

3.1. Руководители отделов

Руководители отделов несут ответственность за обеспечение соблюдения персоналом и другими уполномоченными лицами, работающими в подразделениях, находящихся под их надзором, процедур и принципов, в частности, тех, которые изложены в Условиях использования ИТ-ресурсов.
Они также отвечают за регистрацию информационных ресурсов, находящихся в ведении подразделений, за которые они отвечают, в Инвентаризации информационных ресурсов компании и за назначение пользователя информационного ресурса для каждого из них.

3.2. Пользователи информационных ресурсов

Пользователи информационных ресурсов — это ответственные лица, закрепленные за каждым из информационных ресурсов, перечисленных в Инвентаризации информационных ресурсов компании. Эти пользователи обязаны ежегодно проводить оценку рисков защиты данных, оценивая риски для безопасности и конфиденциальности информационных ресурсов, за которые они несут ответственность, и принимать соответствующие меры по их устранению.

3.3. Наши сотрудники и уполномоченные третьи стороны

Все сотрудники Компании и все третьи лица, уполномоченные Компанией на доступ к информационным ресурсам, обязаны соблюдать положения, изложенные в настоящей Политике. Перед использованием присвоенных им имен пользователей в соответствии с Условиями использования ИТ-ресурсов все сотрудники обязаны принять условия, указанные в вышеупомянутом разделе, которые будут отображаться на их экранах. В случае случайного разглашения или потери данных, несанкционированного доступа, компьютерных вирусов, вредоносного ПО или любого другого инцидента, ставящего под угрозу информационную безопасность, или при подозрении на такие инциденты, о ситуации необходимо немедленно сообщить ИТ-менеджеру. Соответствующие лица могут напрямую связаться с ИТ-менеджером или его сотрудниками для этой цели. (Контактная информация приведена в Разделе 7.1.)

3.4. IT-менеджер

Менеджер по информационным технологиям отвечает за надзор за ресурсами информационных и коммуникационных технологий и выполнение повседневных мероприятий по обеспечению информационной безопасности. ИТ-менеджер может проводить аудит всех используемых систем для выявления и снижения рисков безопасности, а также удалять или отключать имена пользователей/логины, данные и/или программы, признанные небезопасными, на системах, расположенных в сети.

4. СОБЛЮДЕНИЕ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА

4.1. Компания Kardelen Paint and Chemical Industry Trade Limited обязана соблюдать все применимые турецкие законы и административные правила. В сфере информационной безопасности основными правовыми элементами являются Закон № 5651 о регулировании публикаций в интернете и борьбе с преступлениями, совершаемыми посредством таких публикаций, Закон № 6698 о защите персональных данных и Положение о сетевой и информационной безопасности в секторе электронных коммуникаций.

4.2. Соблюдение вышеупомянутых правовых положений является обязанностью всех пользователей, и в случае несоблюдения может возникнуть индивидуальная ответственность. Если какой-либо сотрудник действует вопреки настоящей Политике или положениям действующего законодательства, могут быть приняты дисциплинарные меры в соответствии с трудовым договором, заключенным с нашей Компанией, и соответствующими Дисциплинарными правилами. Несоблюдение требований нашими поставщиками или подрядчиками может привести к расторжению договора с нами. В некоторых случаях могут быть предприняты юридические действия.

5. Инвентаризация данных компании и влияние на защиту данных. ОЦЕНКА

5.1. Компания Kardelen Paint and Chemical Industry Trade Limited ведет реестр данных, содержащий подробную информацию об источниках данных, используемых в ее организации. Руководители отделов и менеджеры филиалов несут ответственность за назначение пользователя ресурса для каждого источника информации, поддерживаемого их соответствующими подразделениями, и за внесение этой информации в реестр данных компании.

5.2. Ежегодно будет проводиться оценка воздействия на все используемые источники информации в отношении рисков для конфиденциальности и безопасности данных, а также рисков, которые используемые инструменты могут представлять для права человека на неприкосновенность частной жизни. Оценка воздействия также будет проводиться перед использованием новых источников информации. Меры, принятые для смягчения этих рисков для источников, обрабатывающих данные, определенные как особые категории данных, будут указаны в инвентаризации данных.

6. МОНИТОРИНГ ЭЛЕКТРОННОЙ СВЯЗИ

В соответствии со статьей 6 Закона № 5561 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. Это включает, 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.

Это не ограничивается перечисленным. Процедуры проверки будут проводиться в соответствии с Принципами внедрения в области электронных коммуникаций и анализа данных.

7. События, связанные с безопасностью данных

7.1. Если какой-либо пользователь обнаружит или заподозрит нарушение безопасности данных или неправомерное использование информационных ресурсов, нарушающее конфиденциальность, доступность и целостность данных, он должен сообщить об этом в группу поддержки ИТ-отдела.

7.2. В случае нарушения безопасности данных, повлекшего за собой случайное или незаконное уничтожение, потерю, изменение, неэффективный доступ к персональным данным или раскрытие персональных данных неуполномоченным лицам, пользователи обязаны немедленно подготовить и направить уведомление о нарушении безопасности данных, которое входит в состав Плана реагирования на нарушение безопасности данных, сотруднику/менеджеру по вопросам защиты данных.

Контактная информация сотрудника/менеджера по вопросам защиты данных: Kardelen Paint and Chemical Industry Trade Limited Company
Телефон: +90 312 398 11 33
Факс: +90 312 398 09 11
Электронная почта: kvkk@kardelenboya.com.tr

7.3. В случае инцидента, связанного с нарушением безопасности данных, или при подозрении на его возникновение, ИТ-менеджер может незамедлительно принять меры для устранения инцидента или минимизации потенциального ущерба, такие как блокировка доступа пользователей к системе или проверка устройств, подключенных к сети.

7.4. Отказ сообщить об инциденте, связанном с нарушением безопасности данных или утечкой персональных данных, может повлечь за собой расследование в соответствии с дисциплинарными нормами. В случае каких-либо колебаний при сообщении об инциденте можно проконсультироваться с ИТ-менеджером или сотрудником/менеджером по вопросам защиты данных.

8. Обучение по вопросам безопасности данных

8.1. Сотрудники, которые будут впервые использовать ИТ-оборудование, а также третьи лица, уполномоченные на доступ к оборудованию, должны быть ознакомлены с политикой и процедурами информационной безопасности Компании. Кроме того, до предоставления доступа к ИТ-услугам пользователи должны пройти обучение требованиям безопасности своей работы и, в целом, правильному использованию ИТ-ресурсов Компании. Ответственность за обеспечение надлежащего обучения сотрудников и ведение учета пройденного обучения лежит на руководителях. Пользователи должны быть проинформированы о настоящей Политике, включая процедуры отчетности, описанные в Разделе 7.

8.2. Все сотрудники компании пройдут обучение по вопросам информационной безопасности и защиты персональных данных, которое будет проводиться в онлайн-формате или очно. В будущем планируется сделать эти тренинги обязательными.

9. ОЦЕНКА БЕЗОПАСНОСТИ В СФЕРЕ ТРУДОУСТРОЙСТВА

9.1. Роли и обязанности, которые необходимо выполнять в отношении безопасности, как указано в настоящей политике и соответствующих положениях, должны быть включены в должностные инструкции, где это уместно. Сюда следует включить общие обязанности по реализации политики безопасности, а также обязанности по защите конкретных информационных активов или выполнению процессов и мероприятий в области безопасности.

9.2. Поскольку полномочия и обязанности в отношении безопасности данных могут меняться в случае подачи заявлений на работу или смены должности сотрудника, эти вопросы должны оцениваться отделом кадров.

9.3. Сотрудники поставщиков или подрядчиков, а также сторонние пользователи, которые будут использовать информационные системы Компании, обязаны подписывать соглашения о конфиденциальности в рамках своих контрактов, а если они имеют доступ к персональным данным, хранящимся в Компании, они обязаны подписывать соглашения об обмене данными.

10. ЗАЩИТА ДАННЫХ ОСОБОЙ КАТЕГОРИИ

Внедрение Компания приняла более строгие меры безопасности для защиты конфиденциальных персональных данных. раздела 10.1 имеет важное значение.

10.2. Особые категории данных не должны храниться или передаваться через отдельные адреса электронной почты (Gmail, Hotmail и т. д.) или веб-сервисы облачного хранения данных (Google Apps, Dropbox и т. д.), не предоставляемые Компанией.

а для Базы данных и компьютеры, содержащие конфиденциальные данные, должны быть зашифрованы, доступа к данным пользователям необходимо вводить учетные данные (статья 10.3).
По возможности данные следует анонимизировать или псевдонимизировать для защиты личных данных, особенно если речь идет об идентифицируемых данных пациентов/участников.

10.4. Все данные на устройствах, используемых моей компанией, должны быть надежно удалены при их утилизации.

10.5. Файлы данных должны быть зашифрованы как на носителе, где они хранятся, так и во время передачи.

11. Условия использования ИТ-ресурсов

Считается, что любой пользователь ИТ-ресурсов компании принял следующее: 11.1.

Под ИТ-ресурсами понимаются все аппаратные средства, программное обеспечение, услуги и ресурсы, предоставляемые для функционирования Компании. Это включает в себя все компьютерные сети, проводные соединения и т. д.

Беспроводные компьютеры, принтеры, мобильные устройства, устройства хранения данных, аудиовизуальные системы и облачные сервисы считаются ИТ-ресурсами. 11.2.

Каждый пользователь должен понимать и применять данные рекомендации по безопасному использованию ИТ-ресурсов, проходить обучение по вопросам информационной безопасности и быть ознакомлен с Заявлением об информационной безопасности; 11.3.

Использование ИТ-ресурсов компании и предоставление доступа к внешним ресурсам должно ограничиваться исследованиями, обучением, административными и другими разрешенными целями, необходимыми для деятельности компании. Использование ИТ-ресурсов для личной коммерческой деятельности без предварительного разрешения запрещено; 11.4. Деятельность, осуществляемая от имени компании, должна выполняться только с использованием средств обработки информации, предоставляемых компанией. Использование внешних информационных сервисов для ведения бизнеса компании подвергает риску данные компании и поэтому запрещено без достаточного обоснования. Например, вместо Dropbox, OneDrive или почтовых сервисов, таких как Gmail и Hotmail, следует использовать собственную почтовую службу компании. 11.5.

Использование информационных технологий компании в личных целях разрешено только в том случае, если это не препятствует деятельности компании или выполнению обязанностей другими пользователями. Использование сети Wi-Fi компании в развлекательных целях также регулируется этим условием.

Сетевым коммутаторам, распределителям, точкам беспроводного доступа и маршрутизаторам запрещается подключать активные сетевые устройства к сети Компании. Все IP-адреса будут назначаться и управляться исключительно Компанией;

11.7. Сотрудники не могут покидать компанию без предварительного письменного разрешения. Доступ к ИТ-услугам Компании для внешних гостей и т. д. запрещен; 11.8. Каждый пользователь ИТ-ресурсов Компании обязан соблюдать Политику информационной безопасности Компании, включая УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ИТ-РЕСУРСОВ и все соответствующие правовые и иные положения, правила, нормы и нормы практики. В частности, но не ограничиваясь этим, каждый пользователь обязан действовать в соответствии с положениями следующих пунктов:

11.8.1. Не разглашайте никому пароль и имя пользователя, присвоенные вам компанией.

11.8.2. Доступ к ИТ-ресурсам не допускается ни внутри, ни за пределами компании, за исключением случаев, когда это разрешено законом, и доступ к этим ресурсам не допускается для несанкционированных целей другими лицами;

11.8.3. Запрещается использовать или вводить в сеть любые материалы или ресурсы, которые могут привести к несанкционированному доступу, изменению или нарушению работы любых ИТ-ресурсов, например, сканирование портов, внутри компании или за ее пределами; 11.8.4. Запрещается использовать любые материалы или ресурсы, которые могут быть расценены как оскорбительные или наносящие ущерб корпоративной репутации компании.

Изображения или тексты, содержащие порнографические, педофильные, сексистские, расистские, клеветнические, угрожающие, порочащие, незаконные, дискриминационные или связанные с терроризмом визуальные или аудиоматериалы, которые могут причинить вред другим, не должны отображаться, храниться, приниматься или передаваться в системах и файлах; 11.8.5. Запрещается выдавать себя за другое лицо в электронных подписях и/или заголовках, создавать и/или передавать «цепочки», «спам» или «навязчивые» электронные письма, использовать выдачу себя за другое лицо для действий от имени других лиц в электронных коммуникациях, а также создавать ненужные или оскорбительные сообщения;

11.8.6. Все мобильные устройства, используемые для доступа к ресурсам, предоставляемым компанией в рамках ее ИТ-услуг, должны быть зашифрованы с использованием соответствующего программного обеспечения для шифрования и защищены PIN-кодом или паролем;

11.8.7. Все материалы и программное обеспечение предоставлены компанией и третьими лицами. Авторские права будут соблюдаться, и материалы, защищенные авторским правом, включая программное обеспечение и полученные данные, не будут использоваться, загружаться, копироваться, храниться в системе или предоставляться без разрешения правообладателя или в соответствии с условиями лицензии, принадлежащей Компании; 11.8.8. При обработке данных о физических лицах будут соблюдаться положения законодательства о защите данных.

Для надлежащей обработки (т.е. сбора, использования, передачи и уничтожения) данных будет соблюдаться Политика компании по защите данных. 11.8.9. Данные, созданные/принадлежащие пользователям/принадлежащие пользователям, на ИТ-ресурсах компании

Следует отметить, что все хранимые информационные активы могут быть подвергнуты проверке со стороны Компании или правоохранительных органов в случае подозрения на совершение противоправных действий. Если соответствующие данные зашифрованы, пользователь обязан предоставить ключ расшифровки; 11.8.10. Условия лицензирования всех материалов и программного обеспечения, используемых через любую платформу, должны быть определены и соблюдаться соответствующим образом; 11.9. В соответствии со статьей 6 Закона № 5561 о регулировании публикаций в Интернете и борьбе с преступлениями, совершаемыми посредством таких публикаций,

Компания принимает 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. Порядок реализации этих мер будет регулироваться Принципами реализации аудита электронных коммуникаций и данных.

В случаях возникновения или подозрения на возникновение инцидента, связанного с нарушением безопасности данных (статья 11.10), руководитель ИТ-отдела может незамедлительно принять меры для устранения инцидента или минимизации потенциального ущерба, такие как блокировка доступа пользователей к системе или проверка устройств, подключенных к сети.

11.11. Если потребуется дальнейшее расследование, ИТ-отдел свяжется с компанией.

С явного разрешения Совета директоров Компания может принимать необходимые меры для проверки любой системы в своей сети.

11.12. За исключением случаев, предусмотренных действующим законодательством, Компания не несет ответственности за любые убытки, ущерб или неблагоприятные события, возникшие прямо или косвенно в результате использования или невозможности использования любых ИТ-ресурсов, предоставляемых и/или управляемых ею.

11.13. Хотя Компания не несет ответственности за несанкционированный доступ к персональным и другим данным или их изменение.

Хотя поставщик принимает надлежащие меры безопасности против разглашения, уничтожения или случайной потери данных, он не предоставляет пользователю никаких гарантий относительно безопасности, конфиденциальности или целостности данных. 11.14.

Имя, адрес, фотография, семейное положение, адрес электронной почты, имя пользователя, псевдоним, удостоверение личности сотрудника и другая соответствующая информация пользователей будут храниться на компьютерных носителях для использования в других целях, таких как администрирование и мониторинг использования системы.

11.15. Вышеуказанные условия также применяются к использованию сети Компании устройствами, не принадлежащими Компании, такими как персональные ноутбуки и домашние компьютеры, при их прямом подключении к сети Компании и/или через VPN. 11.16.

Нарушение вышеуказанных условий может повлечь за собой дисциплинарные меры, включая приостановку доступа ко всем ИТ-ресурсам Компании на определенные периоды и/или наложение штрафных санкций. В случаях серьезных нарушений Компания оставляет за собой право расторгнуть трудовой договор с соответствующим лицом и возбудить гражданское и уголовное дело против

пользователя. Сотрудники Компании будут выступать в качестве представителей гостей, использующих ИТ-ресурсы Компании и/или интернет-соединение, предоставляемое Компанией. Сотрудники, выступающие в качестве представителей, обязаны контролировать действия своих гостей и нести за них ответственность.