КОНТРОЛЬ ДОСТУПА ПОЛИТИКА

KVKK_P7 ВЕРСИЯ 1.00

Компания KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED

ПОЛИТИКА КОНТРОЛЯ ДОСТУПА

1. Цель и сфера применения

Компания Kardelen Boya внедряет физические и логические средства контроля доступа к сетям, ИТ-системам и сервисам, используемым компанией, для обеспечения детального, поддающегося аудиту и надлежащего доступа пользователей, с уровнями авторизации, скорректированными в соответствии с предоставляемой услугой, а также для обеспечения и поддержания конфиденциальности, целостности и доступности данных в соответствии со своей политикой информационной безопасности.

Контроль доступа направлен на защиту интересов всех авторизованных пользователей ИТ-систем, используемых компанией Kardelen Boya, а также данных, предоставленных третьими лицами, путем создания безопасной, защищенной и доступной рабочей среды.

1.1. Настоящая Политика распространяется на все данные, информацию и системы, принадлежащие или эксплуатируемые компанией Kardelen Boya во всех местах, где предоставляется доступ к ИТ-системам и системам электронной связи, используемым компанией Kardelen Boya. Положения настоящей Политики также распространяются на всех поставщиков, подрядчиков, субподрядчиков, консультантов, волонтеров, персонал, сопровождающий исследовательские работы, студентов-стажеров и временных работников, включая третьих лиц и организации, уполномоченные получать доступ к ИТ-системам и системам электронной связи компании Kardelen Boya. Термины «Пользователь информационных активов» или «Пользователь», используемые в настоящей Политике, охватывают вышеупомянутые группы лиц.

1.2. Общедоступный веб-сайт компании и другая информация, классифицируемая как «Общедоступная». Настоящая Политика не распространяется на системы, находящиеся вне контроля компании Kardelen Boya. Ответственность за привилегированный доступ к системам, ресурсам и приложениям, не находящимся под управлением компании, несет владелец системы, ресурса или приложения, а не компания Kardelen Boya. Процессы авторизации и контроля, связанные с предоставлением доступа к этим ресурсам, являются обязанностью владельцев ресурсов.

2. Определения и роли участников

2.1. Доступ к данным, информации и системам предоставляется только при наличии законной деловой необходимости. Доступ может быть предоставлен только при наличии разрешения владельца информационных активов и при соблюдении всех применимых политик, процедур, принципов и условий. Если пользователю больше не требуется доступ к системе по таким причинам, как изменение должности, выход на пенсию, прекращение трудовых отношений или завершение проекта, все предоставленные права доступа должны быть аннулированы, а право доступа к информации должно быть прекращено.

2.2. Пользовательские привилегии позволяют пользователям получать доступ к определенным действиям других пользователей. или же оно должно быть определено таким образом, чтобы предотвратить доступ субъекта информации к данным или иное вмешательство в них, к которым соответствующий пользователь не предоставил специального разрешения на доступ.

2.3. Права доступа как к физическим, так и к логическим объектам будут предоставляться в соответствии с принципами минимального доступа и необходимости знать информацию.

2.4. Принцип минимального доступа означает, что конкретный Пользователь имеет право только на те права, которые ему предоставлены. Это требует, чтобы пользователь не имел больше прав доступа, чем необходимо для выполнения своих обязанностей. Для эффективного применения принципа минимальных прав доступа необходимо определить характер работы пользователя, установить минимальный набор прав доступа, необходимых для выполнения задачи, и ограничить права доступа, предоставляемые пользователю, этим минимальным набором прав.

Права доступа ко всем системам будут устанавливаться по умолчанию таким образом, чтобы предотвратить несанкционированный доступ пользователей, и будет применяться принцип минимальных привилегий, требующий запрета любых привилегий в информационной системе, которые не были специально разрешены.

2.5. Принцип многоуровневой защиты подразумевает внедрение системы защиты на нескольких уровнях различных типов для обеспечения значительно более надежной защиты. Принцип многоуровневой защиты будет применяться с требованием контроля доступа на каждом уровне системы, включая сеть, аппаратные устройства, системное программное обеспечение, приложения и данные.

2.6. Разделение обязанностей: Если бизнес-процесс включает обработку важной или критически важной для компании информации, система должна предусматривать разделение обязанностей или другие механизмы компенсаторного контроля для пользователей. Эти механизмы контроля должны гарантировать, что ни одно лицо не обладает единоличной властью над информационными активами или связанными с ними функциями. Примером нарушения принципа разделения обязанностей может служить ситуация, когда одно и то же лицо отвечает за выписку чеков и ведение исторических данных, связанных с финансовыми операциями.

По возможности, ни один человек не должен нести единоличную ответственность за выполнение задачи, связанной со специальной, конфиденциальной или критически важной информацией, от начала до конца. Аналогично, ни один человек не должен нести единоличную ответственность за утверждение собственной работы. По возможности, по меньшей мере два человека должны координировать деятельность по обработке информации для каждой задачи.

2.7. Допустимое использование: Укажите Kardelen перед определением имени пользователя и пароля. Каждый пользователь, желающий получить разрешение на подключение к системам, используемым компанией Boya, должен быть проинформирован о Политике допустимого использования ИТ-ресурсов и электронных средств связи, а также подписать Декларацию о повышении осведомленности в вопросах информационной безопасности.

2.8. Все третьи стороны, имеющие доступ к данным, информации и системам компании, обязаны воздерживаться от разглашения любой информации, которую Kardelen Boya считает не подлежащей публичному разглашению. Для третьих сторон, привлеченных по контракту, заказу на закупку или субподрядному соглашению, во все контракты и заказы на закупку между Kardelen Boya и третьей стороной, получившей доступ к данным, информации и системам Kardelen Boya, будет включено стандартное положение о конфиденциальности. Письменное соглашение о конфиденциальности будет заключено со всеми физическими или юридическими лицами, предоставляющими услуги Kardelen Boya (требующие доступа к конфиденциальным данным), но не имеющими контракта с Kardelen Boya.

2.9. Контроль доступа: Контроль доступа — это любой механизм, обеспечивающий доступ к данным. Для доступа к компьютерам пользователь должен сначала войти в систему, используя соответствующий метод аутентификации. Механизм контроля доступа сравнивает имя пользователя, присвоенное пользователю, со списком контроля доступа.

Система определяет, какие задачи и операции может и не может выполнять соответствующий пользователь.

Системы контроля доступа включают следующие элементы: • Создание,

чтение, редактирование или удаление файлов на файловом сервере и т. д.

права доступа к файлам

• Программы, такие как право запуска определенной программы на сервере приложений.

разрешения

• Права на данные, такие как извлечение данных из базы данных или обновление информации.

Процедуры контроля доступа представляют собой совокупность методов и практик, используемых владельцами информационных активов для предоставления пользователям доступа к данным, информации или системам.

2.10. Аутентификация: Аутентификация — это процесс проверки учетных данных пользователя информации владельцем информационных активов, уполномоченным идентифицировать этого пользователя. В компьютерных системах аутентификация обычно выполняется с использованием уникальной комбинации имени пользователя и пароля, известной только пользователю информации и определенной для этого пользователя. Использование других методов аутентификации может быть разрешено генеральным директором по рекомендации ИТ-менеджера и консультанта по GDPR. 2.11.

Система: Система — это набор информационных ресурсов, взаимосвязанных под одним и тем же непосредственным регулирующим контролем и обладающих общей функциональностью. Система может состоять из аппаратного обеспечения, программного обеспечения, информации, данных, приложений или коммуникационной инфраструктуры. Корпоративная система, с другой стороны, — это системы, которые обрабатывают информацию для поддержки текущих бизнес-процессов. Для систем, отнесенных к корпоративным системам, требования к безопасности будут определяться в соответствии с бизнес-требованиями. 2.12.

Индивидуальная ответственность: Каждый пользователь несет индивидуальную ответственность за доступ к электронным ресурсам, предоставляемым и используемым компанией Kardelen Boya. Для доступа к компьютерным системам и сетям требуется использование уникальных учетных данных, присваиваемых каждому пользователю индивидуально и известных как имя пользователя. Каждый пользователь ИТ-инструментов Kardelen Boya имеет доступ только к тем ресурсам, к которым он имеет право. Для аутентификации пользователя при доступе к данным, информации или системе требуется использование смарт-ключа, аналогичного паролю для входа в систему. Информация о паролях считается конфиденциальной и не должна разглашаться никому. Каждый пользователь несет ответственность за принятие разумных мер безопасности для предотвращения несанкционированного использования информации о своих паролях. Для получения подробной информации см.: Положение о процедурах и принципах определения, использования и защиты пользовательских паролей.

2.13. Владельцы информационных активов: Владельцы информационных активов несут ответственность за определение того, кто может получить доступ к защищенным ресурсам и какие права доступа будут установлены (чтение, обновление и т. д.). Эти права доступа должны соответствовать обязанностям и ответственности пользователя информации. Владельцы информационных активов могут делегировать часть своих административных обязанностей подчиненным, но в конечном итоге они несут ответственность за сами информационные

активы. 2.14. Руководители отделов: Руководители отделов играют ведущую роль в обеспечении информационной безопасности в компании Kardelen Boya. Руководители отделов получают доступ к системе от имени пользователей информации, когда доступ необходим для выполнения бизнес-процессов.

Они отвечают за документирование запросов. Руководители отделов несут ответственность за изменение и/или отзыв прав доступа пользователей в случае изменения должностных обязанностей или статуса пользователя информации.

3. РУКОВОДСТВО ПО ПРОЦЕДУРАМ КОНТРОЛЯ ДОСТУПА

3.1. Компания Kardelen Boya предоставит всем своим сотрудникам и сторонним поставщикам соответствующие права доступа к данным, находящимся в ее ведении, чтобы обеспечить максимально эффективное выполнение ими возложенных на них обязанностей.

3.1.1. Общие идентификаторы пользователей: как правило, это общие или групповые учетные данные.

Идентификация и использование данных Карделена Боя не допускается, но может быть разрешено в исключительных случаях при наличии надлежащих механизмов контроля.

3.1.2. При любых обстоятельствах поставщиком интернет-услуг будет компания Kardelen Boya.

Для выполнения своих юридических обязанностей и обеспечения соблюдения положений Политики надлежащего использования электронных ресурсов, личности пользователей, обладающих корпоративной идентификационной информацией, должны быть идентифицируемыми. Идентификационные данные обычных пользователей ни при каких обстоятельствах не могут быть использованы для доступа к конфиденциальной или секретной информации.

3.1.3. Учетные записи с привилегированными правами доступа: Назначение привилегированных прав доступа, таких как локальный администратор, администратор домена, суперпользователь и администратор, будет ограничено пользователями, которых сочтет подходящими высшее руководство, и не может быть определено по умолчанию.

3.1.3.1. Разрешение на использование таких счетов будет предоставлено и задокументировано только Генеральным директором по письменному запросу старшего руководителя (начальника отдела, заместителя Генерального директора).

3.1.3.2. Технические группы будут принимать меры предосторожности, чтобы не предоставлять преференциальные права всем группам во избежание потенциальной потери конфиденциальности и/или целостности данных.

3.1.3.3. Привилегированные учетные записи не должны использоваться для рутинных действий; Программа

Данные определения могут использоваться только для установки программы и перенастройки системы, а не для использования самой программы, если только ее работа не является невозможной иным способом.

3.1.4. Принцип минимальных привилегий и что вам нужно знать: как физические, так и...

Права доступа к логическим объектам будут предоставляться в соответствии с принципами минимального доступа и информацией, которую вам необходимо знать.

3.2. Авторизация контроля доступа 3.2.1. Учетные записи пользователей: доступ к ИТ-ресурсам и услугам, используемым компанией Kardelen Boya

Доступ будет предоставлен после ввода исходной учетной записи пользователя и сложного пароля.

3.2.2. Учетные записи пользователей предоставляются на основании наличия действительной записи о сотруднике в системе управления персоналом. Для любого пользователя, не имеющего записи о сотруднике, разрешение на доступ предоставляется руководителем отдела. Доступ по умолчанию предоставляется только для доступа к определенному разделу, носителю информации и учетной записи электронной почты.

3.2.3. Доступ к конфиденциальной информации, информации с ограниченным доступом и информации, необходимой для использования только в рамках конкретного подразделения: уполномоченные лица, которым необходим доступ к соответствующей информации в связи с выполнением служебных или рабочих обязанностей в соответствии с действующим законодательством и соглашениями с соответствующими сторонами.

Доступ к рассматриваемой информации будет ограничен сотрудниками. Ограничение доступа к рассматриваемой информации будет осуществляться с помощью межсетевых экранов, сетевой изоляции, безопасных процедур входа в систему, ограничений по спискам контроля доступа и других мер, которые будут сочтены целесообразными. Ответственность за внедрение ограничений доступа лежит на руководителях подразделений и ИТ-отделе, обрабатывающем соответствующую информацию, и будет осуществляться в соответствии с положениями настоящей Политики. Для обеспечения безопасного доступа ко всем файловым ресурсам, расположенным в доменах Active Directory компании Kardelen Boya и управляемым ими, будут применяться методы контроля доступа на основе ролей.

3.3. Проверка личности и аутентификация: Все компьютеры, подключенные к сети Kardelen Boya, должны быть оснащены механизмами аутентификации, такими как имена пользователей и пароли, для обеспечения контроля доступа. В многопользовательских системах для каждого пользователя должны быть уникальные имена пользователей и пароли, а также механизмы ограничения прав доступа пользователей. Программные и аппаратные средства контроля для предотвращения несанкционированного доступа на всех рабочих станциях, независимо от состояния доступа к сети, будут внедрены и утверждены ИТ-менеджером.

3.4. Все пользователи обязаны подтвердить свою личность перед доступом к любой информации, данным или системам. Необходимо соблюдать процедуры верификации. Для этого перед предоставлением доступа к внутренним сетям компании потребуется имя пользователя и пароль, уникальные для каждого пользователя.

3.5. Пользователям следует воздерживаться от использования имен пользователей и паролей, которые они используют для доступа к системным и вычислительным ресурсам, используемым компанией Kardelen Boya, для доступа к системам за пределами компании Kardelen Boya, включая учетные записи, используемые ими в Интернете.

3.6. В сетевых компьютерных системах на экране входа пользователя должно отображаться следующее:
Система будет содержать информацию, запрашивающую у пользователя ввод имени пользователя и пароля для входа в систему. Информация о компьютере, операционной системе, конфигурации сети или другая информация, относящаяся к конкретной компании, ни в коем случае не должна передаваться пользователю до тех пор, пока он не войдет в систему, используя действительное имя пользователя и пароль. Если какой-либо из шагов входа в систему будет выполнен неправильно, пользователь получит только уведомление о неудачной попытке входа, без объяснения причины проблемы.

3.7. Уникальные имена пользователей: Каждое имя пользователя должно быть уникальным для пользователя, которому оно назначено, и должно быть связано только с этим пользователем. Если права доступа пользователя к системе прекращаются, имя пользователя этого пользователя никогда не должно использоваться повторно. Каждое имя пользователя и пароль должны быть определены для исключительного использования конкретным лицом. Имена пользователей могут передаваться по электронной почте и в других средствах массовой информации, но пароли никогда не будут передаваться никому ни в каком виде. (У группы ИТ-поддержки есть собственные права доступа, и ей не нужен доступ к паролям пользователей.)

3.8. Процедуры аутентификации пользователей: Все корпоративные информационные системы гарантируют, что только авторизованные пользователи могут использовать имена пользователей с заданными паролями или более надежными методами динамического шифрования. Пользователи несут личную ответственность за все действия и транзакции, выполняемые в сессиях, открытых с использованием имен пользователей и паролей или других механизмов аутентификации. Пользователи обязаны немедленно сменить свои пароли, если обнаружат, что их учетные данные были раскрыты или использованы третьими лицами. Аналогичным образом, пользователи несут ответственность за контроль доступа с использованием информации о сессиях.

Если пользователи подозревают, что конфиденциальность их механизмов была нарушена, они обязаны немедленно сообщить об этом в техническое подразделение ИТ-отдела. Имена пользователей могут использоваться только назначенным персоналом. Пользователи ни в коем случае не должны позволять другим лицам совершать какие-либо действия, используя их имя пользователя. Аналогично, пользователи не могут совершать какие-либо действия или транзакции, используя имена пользователей, назначенные другим пользователям.

3.9. ПОРТАТИВНЫЕ КОМПЬЮТЕРЫ И ДРУГИЕ УСТРОЙСТВА: Конфиденциальные или важные данные не могут храниться на портативных ноутбуках, iPad, нетбуках, портативных компьютерах и аналогичных устройствах, если они не защищены описанными выше процессами авторизации. Пользователи несут личную ответственность за физическую безопасность этих устройств и конфиденциальность информации и документов, содержащихся в них.

3.10), ПОРТАТИВНЫЕ УСТРОЙСТВА ПАМЯТИ: Если информация, не разглашаемая компанией публично (пункт записывается на мягкие диски, магнитные ленты, смарт-карты или другие носители информации, указанные носители должны быть помечены в соответствии с наивысшим уровнем конфиденциальности. В нерабочее время носители информации должны храниться в безопасном месте.

Операции удаленной записи: Необходимо внедрить необходимые меры контроля для предотвращения несанкционированного доступа к конфиденциальным или частным данным (данным, указанным в разделе 3.11) во время операций удаленной записи. Пользователи должны обеспечить печать конфиденциальной информации на защищенном принтере или проведение процесса печати под наблюдением уполномоченного лица, имеющего право просматривать распечатанные материалы.

ОБМЕН И ПЕРЕДАЧА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ И ДАННЫХ ОСОБОЙ КАТЕГОРИИ: 3.12. Пользователям запрещается устанавливать соединения с электронными носителями памяти, локальными сетями, серверами передачи файлов (FTP), веб-серверами или модемами к существующим локальным сетям или другим многопользовательским системам с целью передачи информации без предварительного разрешения ИТ-отдела. Устанавливать такие соединения разрешено только персоналу, специально уполномоченному ИТ-менеджером и обладающему особыми правами доступа.

3.13. УТИЛИЗАЦИЯ И ПЕРЕРАБОТКА ОБОРУДОВАНИЯ И СРЕДЫ ХРАНЕНИЯ

ИЗЪЯТИЕ: Если компьютерные носители информации отправляются поставщику для замены, обслуживания или уничтожения, все конфиденциальные и служебные данные будут уничтожены или скрыты с использованием утвержденных методов.

ПРИОСТАНОВЛЕНИЕ И ОТМЕНА ПРАВ ДОСТУПА: 3.14.

3.14.1. Доступ пользователей к информационным активам, находящимся в распоряжении владельцев информационных активов. Владелец данных несет ответственность за установление применимых правил отзыва прав доступа. Назначенные владельцем данных сотрудники будут осуществлять процессы предоставления и отзыва прав доступа пользователям от имени владельца данных в соответствии с установленными правилами.

3.14.2. Руководители отделов обязаны незамедлительно сообщать о любых изменениях в назначении пользователей или статусе занятости, требующих внесения изменений в предоставленные им права доступа. В случае прекращения трудовых отношений менеджер по персоналу будет управлять процессом отзыва прав доступа соответствующего пользователя ко всем данным, информации и системам и уведомит об этом ИТ-менеджера.

3.14.3. Руководители отделов несут ответственность за ежегодный пересмотр и обновление системы прав доступа, предоставляемых пользователям. В случае изменения прав доступа пользователей руководители отделов внесут необходимые детальные изменения в механизм управления учетными записями пользователей.

3.14.4. В случае прекращения отношений пользователя с компанией Kardelen Boya, соответствующий руководитель отдела незамедлительно проверит внутренние файлы компьютера и бумажные файлы, хранящиеся вручную, чтобы определить, кто будет нести ответственность за их хранение и/или определить соответствующие методы их уничтожения. Впоследствии руководитель отдела должен пересмотреть обязанности пользователя компьютера, конкретно делегировав ответственность за файлы, ранее закрепленные за этим пользователем, новому назначенному пользователю. 3.14.5. Учетные записи пользователей, не проявлявших никакой активности в течение трех месяцев, будут автоматически приостановлены. Права доступа для пользователей, возобновивших свою работу после отпуска, временного назначения или неоплачиваемого отпуска, превышающего один месяц, будут переопределены соответствующим руководителем отдела.

3.14.6. Сеанс: Если в течение двадцати минут на рабочей станции не наблюдается никакой активности, система должна автоматически затемнить экран и завершить сеанс. Повторный вход в сеанс должен быть разрешен только после того, как пользователь введет свой действительный пароль. 3.14.7. Управление паролями: Пароли, списки контроля доступа и другая информация о контроле доступа должны быть зашифрованы при хранении или передаче по сети. Должны быть приняты необходимые меры контроля для предотвращения несанкционированного доступа и использования хранимых паролей и информации о контроле доступа. 3.14.8. Пароли не должны быть напрямую встроены (закодированы) в программное обеспечение или приложения, чтобы обеспечить возможность их изменения при необходимости.

3.14.9. Пароли, выданные новым пользователям, должны быть действительны только для первого входа пользователя в систему. После входа в систему пользователь должен установить новый пароль. Та же процедура применяется к сбросу пароля, если пользователь забыл свой пароль.

3.14.10. Пароли по умолчанию на устройствах, полученных от поставщиков, необходимо изменить до первого использования оборудования. Эта процедура распространяется как на учетные данные конечного пользователя, так и на учетные данные системного администратора и других привилегированных пользователей.

3.14.11. Пользователи не должны передавать пароли от своих индивидуальных учетных записей никому, включая руководителей подразделений и коллег. Для обмена файлами и информацией пользователи должны использовать общие каталоги локальной сети, электронную почту, страницы интранета или дисководы для гибких дисков — механизмы, одобренные и разрешенные ИТ-отделом.

3.14.12. Разработка системы: Описанные ниже стандарты будут использоваться для предотвращения несанкционированного доступа персонала к данным, созданным компанией, и для повышения целостности приложений.

Разделение корпоративных данных, систем разработки и тестирования: данные, генерируемые в конечном итоге корпоративными бизнес-процессами, должны быть отделены от сред разработки и тестирования. Это обеспечивает лучшую защиту корпоративной информации.

Персоналу, работающему в средах разработки и тестирования, в принципе, не разрешен доступ к корпоративным системам. Только руководители отделов могут разрешить сотрудникам отдела разработки доступ к корпоративным данным. Аналогичным образом, все подразделения корпоративного тестирования программного обеспечения должны обрабатывать удаленные данные, заменяя конфиденциальную и служебную информацию и данные поддельными данными. Корпоративные системы и информация

Для ограничения и утверждения изменений следует использовать формальные и документированные процессы управления изменениями.

Разработка программного обеспечения: Прежде чем программное обеспечение будет развернуто для использования в корпоративной среде, разработчики программ и другой технический персонал должны исключить все частные пути доступа, чтобы гарантировать, что доступ возможен только обычными, безопасными способами. Следовательно, необходимо удалить все скрытые программы доступа и другие средства, которые могут быть использованы для компрометации безопасности системы. Все процедуры контроля доступа на уровне пользователей и администраторов, предусмотренные в политиках и правилах информационной безопасности, должны быть определены и активированы до развертывания разработанных систем для корпоративного использования.

Контроль миграции среды: После завершения этапов разработки и тестирования программного обеспечения необходимо внедрить соответствующую методологию, чтобы обеспечить упорядоченный и контролируемый процесс миграции программного обеспечения на корпоративные платформы. Персонал, занимающийся разработкой приложений, не должен иметь прямого доступа к загрузке программного обеспечения в корпоративную ИТ-среду. Должны быть внедрены необходимые меры контроля для предотвращения миграции несанкционированного кода приложений в корпоративную ИТ-среду.

Права доступа, вносящие изменения в процессы производства корпоративных знаний, должны ограничиваться приложениями для производства корпоративных знаний. При определении прав доступа пользователям системы не следует разрешать изменять системные данные без ограничений. Пользователи должны использовать корпоративные данные для укрепления и защиты целостности систем.

Они должны иметь возможность вносить изменения только в ранее определенные форматы. Обновление корпоративных баз данных должно выполняться с использованием утвержденных руководством методов. Использование инструментов прямого доступа к базам данных в корпоративной информационной среде недопустимо, поскольку эти программы могут нарушать процедуры синхронизации и репликации баз данных, процедуры обработки ошибок ввода и другие критически важные механизмы управления.

Журналы событий и другие инструменты безопасности: Компьютерные и коммуникационные системы, содержащие конфиденциальные или важные данные, должны регистрировать все значимые события безопасности. Примеры событий безопасности включают: изменение учетных данных пользователями во время онлайн-сессий, попытки подбора паролей, попытки использования несанкционированных прав доступа, модификации корпоративного прикладного программного обеспечения, изменения системного программного обеспечения, изменяющие права пользователей, и модификации подсистем ведения журналов.

ИТ-менеджер будет регулярно отчитываться перед высшим руководством о событиях, происшествиях, уровне соответствия политикам, изменениях и других вопросах, связанных с безопасностью доступа.

Требования к отчетности: О несанкционированном доступе или попытке доступа, краже или разглашении паролей или средств контроля доступа, предполагаемой потере, изменении или разглашении данных, а также о нарушениях стандартов, процедур или политик безопасности необходимо немедленно сообщать ближайшему руководителю подразделения или группе технической поддержки ИТ, заполнив форму, включенную в План реагирования на утечку данных.

4. Физический контроль доступа: В связи с конфиденциальностью ресурсов и данных, хранящихся на объектах, используемых компанией Kardelen Boya, в случае ограничений доступа контроль доступа будет осуществляться преимущественно с использованием технологии RFID.

Это будет предоставляться посредством идентификационных карт. Данные из системного помещения и отдела исследований и разработок. Системы распознавания отпечатков пальцев также могут использоваться для доступа в зону при условии получения предварительного письменного разрешения от генерального директора. Системы распознавания карт и отпечатков пальцев могут использоваться только для предоставления доступа в зоны, доступ в которые ограничен для уполномоченного персонала, и категорически не могут использоваться для контроля за соблюдением персоналом рабочего времени.

4.1. В случае утери удостоверения личности Kardelen Boya необходимо немедленно сообщить об этом в ИТ-отдел. Ответственное лицо уведомляется. IT-менеджер незамедлительно обеспечивает удаление соответствующей карты из системы контроля физического доступа компании. Новая карта будет выдана только после аннулирования утерянной карты. Новая карта будет иметь те же права доступа, что и старая.

4.2. Данные, хранящиеся в системах контроля доступа: Компания хранит следующие данные о своей системе контроля доступа: • Данные владельца карты: о Имя и фамилия

Должность, отдел, адрес электронной почты, регистрационный номер сотрудника, номер мобильного телефона.

• Карты, выданные держателю карты

• Место, дата и время проведения операции считывания карты

4.2.1. Доступ к данным контроля доступа могут иметь сотрудники, чьи должностные обязанности требуют доступа к программному обеспечению контроля доступа. К таким сотрудникам относятся:

• Охранники • Технический персонал, выдающий карты доступа или выполняющий процедуры замены и уничтожения карт

• Специалисты технической поддержки ИТ

4.2.2. В случаях, когда данные должны быть переданы из системы контроля доступа запрашивающему получателю, В соответствии с процедурами, изложенными в настоящей Политике, по мере возможности следует удалять все поля, позволяющие идентифицировать данные как принадлежащие конкретному лицу. Например, если необходимо узнать, сколько человек использовали считыватель за определенный период, в отчете не потребуется раскрывать имена, фотографии или другую личную информацию держателей карт; будут передаваться только данные, относящиеся к процессу считывания карты.

4.3. Методы контроля доступа

Доступ к данным обеспечивается различными способами с использованием методов, перечисленных ниже, в соответствии с уровнями классификации данных.

В качестве методов контроля доступа по умолчанию используются следующие:

• Откройте страницу входа в систему на устройствах.

• Настройка общего доступа и прав доступа к файлам и папкам в Windows.

• Ограничения прав доступа к учетной записи пользователя,

- Права доступа к серверу и рабочим станциям,
- Разрешения брандмауэра,
- Списки контроля доступа к сетевым зонам и VLAN,
- Права аутентификации в интранете/экстранете
- Права доступа пользователя Kardelen Boya,
- Права доступа к базе данных и списки контроля доступа,
- Шифрование данных в состоянии покоя и в процессе передачи.
- Другие методы, предусмотренные договором и требуемые соответствующими сторонами.

4.4. Контроль доступа распространяется на все сети, серверы и рабочие станции, принадлежащие компании Kardelen Boya. Это относится к ноутбукам и мобильным устройствам.

4.5. В качестве метода обеспечения безопасности доступа ко всем файловым ресурсам, расположенным в доменах Active Directory компании Kardelen Boya, будет использоваться управление доступом на основе ролей.

4.6. Тестирование на проникновение: Механизм контроля доступа Kardelen Boya будет регулярно проходить тестирование на проникновение для определения эффективности существующих средств контроля и выявления любых слабых мест. В соответствующих случаях и по согласованию эти тесты будут также включать системы поставщиков облачных услуг.

Запросы, касающиеся данных контроля доступа.
ТЕКУЩИЙ ПРОЦЕСС