УТВЕРЖДАЮ
Генеральный директор
«Кузбасс-пригород»
АО _____П.В.Кутловский
«24» апреля 2021 г.

Политика информационной безопасности АО «Кузбасс-пригород»

1. Общие положения

Политика информационной безопасности АО «Кузбасс-пригород» (далее – Общество) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее - ИБ), которыми руководствуются работники Общества при осуществлении своей деятельности.

Основной целью Политики информационной безопасности АО «Кузбасс-пригород» является защита информации Общества при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.

Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным закон от 6 апреля 2011г. № 63-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №1119 от 01.11.12г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ №687 от 15.09.08г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» а также рядом иных нормативных правовых актов в сфере защиты информации.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Общества. На лиц, работающих по договорам гражданско-правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

2. Цели и задачи политики информационной безопасности

Основными целями политики ИБ являются:

сохранение конфиденциальности информационных ресурсов; обеспечение непрерывности доступа к информационным ресурсам;

защита целостности информации с целью поддержания возможности Общества по оказанию услуг высокого качества и принятию эффективных управленческих решений;

повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами;

определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;

предотвращение и/или снижение ущерба от инцидентов ИБ.

Основными задачами политики ИБ являются:

разработка требований по обеспечению ИБ;

контроль выполнения установленных требований по обеспечению ИБ;

повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;

разработка нормативных документов для обеспечения ИБ Общества;

выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ Общества;

организация антивирусной защиты информационных ресурсов Общества;

защита информации Общества от несанкционированного доступа (далее НСД) и утечки по техническим каналам связи.

3. Обеспечение информационной безопасности

Политика ИБ Общества направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников Общества, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

Наибольшими возможностями для нанесения ущерба обладает персонал Общества. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их

способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Стратегия обеспечения ИБ Общества заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников Общества.

4. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются:

постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов Общества;

своевременное обнаружение проблем, потенциально способных повлиять на ИБ Общества,

корректировка моделей угроз и нарушителя;

разработка и внедрение защитных мер;

контроль эффективности принимаемых защитных мер;

персонификация и разделение ролей и ответственности между сотрудниками Общества за обеспечение ИБ исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты

Объектами защиты с точки зрения ИБ в управлении являются:

информационный процесс профессиональной деятельности;

информационные активы Общества.

Защищаемая информация делится на следующие виды:

информация по финансово-экономической деятельности Общества;

персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6.Требования по информационной безопасности

В отношении всех собственных информационных активов, находящихся под контролем Общества, а также активов, используемых для получения доступа

к инфраструктуре Общества, должна быть определена ответственность соответствующего сотрудника Общества. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами Общества должна доводиться до сведения генерального директора Общества.

Все работы в пределах Общества должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.

Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

сотрудникам Общества разрешается использовать сеть Интернет только в служебных целях;

запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

работа сотрудников Общества с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Общества в сеть Интернет;

сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Общества;

сотрудники Общества перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

запрещен доступ в Интернет через сеть Общества для всех лиц, не являющихся сотрудниками Общества, включая членов семьи сотрудников.

Системный администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Общества.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит системный администратор.

Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное Обществом, является ее собственностью и предназначено для использования исключительно в производственных целях.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к системному администратору. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

Порты передачи данных, в том числе CD дисководы в стационарных компьютерах сотрудников Общества блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

Все программное обеспечение, установленное на предоставленном Обществом компьютерном оборудовании, является собственностью Общества и должно использоваться исключительно в производственных целях.

Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственно генеральному директору Общества.

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации: персональный межсетевой экран; антивирусное программное обеспечение.

Сотрудники Общества не должны:

блокировать антивирусное программное обеспечение;

устанавливать другое антивирусное программное обеспечение;

изменять настройки и конфигурацию антивирусного программного обеспечения.

Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию Общества по электронной почте без использования систем шифрования. Строго конфиденциальная информация Общества, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Использование сотрудниками Общества публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.

Сотрудники Общества для обмена документами должны использовать только свой официальный адрес электронной почты.

Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения

сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.

Не допускается при использования электронной почты:

рассылка сообщений личного характера,

использующих значительные ресурсы электронной почты;

рассылка рекламных материалов;

подписка на рассылку,

участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить администратору и генеральному директору Общества.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

проинформировать администратора;

не использовать и не включать зараженный компьютер;

не подсоединять этот компьютер к компьютерной сети Общества до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.

Сотрудникам Общества запрещается:

нарушать информационную безопасность и работу сети Общества;

сканировать порты или систему безопасности;

контролировать работу сети с перехватом данных;

получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

передавать информацию о сотрудниках или списки сотрудников Общества посторонним лицам;

создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Все заявки на проведение технического обслуживания компьютеров должны направляться системному администратору.

7. Управление информационной безопасностью

Управление ИБ Общества включает в себя:

разработку и поддержание в актуальном состоянии Политики информационной безопасности;

разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;

обеспечение бесперебойного функционирования комплекса средств ИБ;

оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

Реализация Политики ИБ Общества осуществляется на основании документов, регламентирующих отдельные процедуры и процессы деятельности Общества.

9. Порядок внесения изменений и дополнений в политику информационной безопасности

Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10. Контроль за соблюдением политики информационной безопасности

Текущий контроль за соблюдением выполнения требований Политики информационной безопасности Общества возлагается на начальника технического отдела.

Генеральный директор Общества на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.