УТВЕРЖДАЮ
Директор ГАПОУ «ОГК»
_____ И.Г.Золкина
«23» октября 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ОГК-П-235-18

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГАПОУ «ОГК»

Версия 01

Дата введения: «23» октября 2018 г.

г.Оренбург, 2018 г.

1. Общие положения

Настоящая политика информационной безопасности разработана в соответствии с требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", гражданского законодательства.

Политика информационной безопасности 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 ГАПОУ «ОГК».

Ответственность за соблюдение информационной безопасности несет каждый сотрудник колледжа, при этом первоочередной задачей является обеспечение безопасности всей информации, касающейся колледжа. Это значит, что информация должна быть защищена не менее надежно, чем любое другое имущество колледжа. Главные цели колледжа не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники колледжа. На лиц, работающих в колледже по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

1.1. Цель и назначение настоящей Политики
Целями настоящей Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам колледжа для поддержки деятельности;
- защита целостности информации с целью поддержания возможности колледжа по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами колледжа;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в колледже.

Руководители подразделений колледжа должны обеспечить регулярный контроль за соблюдением положений настоящей Политики.

1.2. Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации колледжем. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации колледжа, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

Колледжу принадлежит на праве собственности (оперативном управлении) (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования колледжа, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала колледжа.

2. Требования и рекомендации

2.1. Ответственность за информационное имущество

В отношении всего информационного имущества колледжа, находящегося под контролем колледжа, а также имущества, используемого для получения доступа к инфраструктуре колледжа, должна быть определена ответственность соответствующего сотрудника колледжа.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения

Под информационными системами в настоящем положении подразумеваются все информационные системы, как закрытые, так и открытые, используемые в колледже.

Открытая информационная система – «общий доступ» или «корпоративная сеть» доступна только для сотрудников колледжа.

Все работы в открытых и закрытых системах проводятся в пределах помещений колледжа и выполняются в соответствии с официальными должност-

ными обязанностями только на компьютерах, разрешенных к использованию в колледже.

В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в закрытую 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, если работа выполняется дома.

2.2.2. Доступ третьих лиц к системам колледжа

Каждый сотрудник обязан немедленно уведомить сотрудника ответственного за информационную безопасность обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам колледжа должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам колледжа должен быть четко определен, контролируем и защищен.

2.2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам колледжа с учетом их взаимоотношений с колледжем.

Сотрудникам, использующим в работе портативные компьютеры колледжа, может быть предоставлен удаленный доступ к сетевым ресурсам колледжа в соответствии с правами в информационной системе.

Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам колледжа, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети колледжа и к каким-либо другим сетям, не принадлежащим колледжу.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети колледжа, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

2.2.4. Доступ к сети Интернет

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

Рекомендованные правила:

- сотрудникам колледжа разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию, запрещенную к использованию или распространению законодательством РФ;
- сотрудники колледжа не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников колледжа с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации колледжа в сеть Интернет;
- сотрудники колледжа перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

Сотрудник ответственный за информационную безопасность имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

2.3. Защита оборудования

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация колледжа.

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят специалисты отдела информационных технологий.

2.3.1. Аппаратное обеспечение

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 колледжем, является его собственностью (на праве оперативного управления) и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну или иную тайну, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего

стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

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

Все компьютеры должны защищаться паролем при загрузке системы. Для установки режимов защиты пользователь должен обратиться к сотруднику ответственному за информационную безопасность. 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 его контрагентам или партнерам 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.

2.3.2. Программное обеспечение

Все программное обеспечение, установленное на предоставленном колледжем компьютерном оборудовании, является собственностью (на праве оперативного управления) колледжа 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 непосредственному руководителю сотрудника и директору колледжа.

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты.

Сотрудники колледжа не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

2.4. Рекомендуемые правила пользования электронной почтой
Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены третьими лицами для их использования в качестве доказательств в процессе судебного разбирательства или использования в своей деятельности. Поэтому содержание электронных сообщений должно строго соответствовать нормам деловой этики.
Сотрудники колледжа для обмена документами с партнерами должны использовать только свой официальный адрес электронной почты, либо электронную почту ogppk@mail.ru

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.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем пользователям колледжа сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью колледжа;

- 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 нормам в области этики.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в колледже процедурами документооборота.

Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры колледжа для других пользователей. Не желателен объем вложений превышающий 2 Мбайт.

2.5. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

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, либо любого другого компьютерного оборудования следует незамедлительно сообщить об инциденте сотрудникам отдела информационных технологий, своему непосредственному руководителю, директору колледжа.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Не-

обходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

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

- проинформировать сотрудников отдела информационных технологий;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети колледжа до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование сотрудниками отдела информационных технологий.

2.6. Помещения с техническими средствами информационной безопасности
Конфиденциальные встречи (заседания, совещания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.
Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с сотрудником ответственным за информационную безопасность.

Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник колледжа, который отвечает за подготовку заседания, после получения письменного или устного разрешения директора.

2.7. Управление сетью
Сотрудники отдела информационных технологий контролируют содержание всех потоков данных проходящих через сеть колледжа.
Сотрудникам колледжа запрещается:

- нарушать информационную безопасность и работу сети колледжа;
- 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;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

- передавать информацию о сотрудниках или списки сотрудников колледжа посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

2.7.1. Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Специалисты отдела информационных технологий обязаны оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.
Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

Только специалисты отдела информационных технологий на основании заявок руководителей подразделений могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

Все заявки на проведение технического обслуживания компьютеров должны направляться в отдел информационных технологий.

2.8. Разработка систем и управление внесением изменений

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и выполняются специалистами отдела информационных технологий.
Технические средства информационных систем используемых колледжем находятся на территории Российской Федерации.

Лист регистрации изменений

№ изме-нения	**Дата внесения изменения, дополнения**	**Номера листов**	**Краткое содержание изменения**	**Ф.И.О., должность, подпись лица, осуще-ствившего изменение документа**
1	**2**	**3**	**4**	**5**