УТВЕРЖДАЮ
Директор УО «Пинский государственный аграрно-технический
колледж имени А.Е.Клещёва»
_____И.М. Колб
«__»_____ 2022г.

ПОЛИТИКА
информационной безопасности

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности в учреждении образования «Пинский государственный аграрно-технический колледж имени А.Е.Клещева» (далее - Политика) определяет общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, в том числе и персональных данных, документально закрепленные собственником информационной системы учреждения образования «Пинский государственный аграрно-технический колледж имени А.Е.Клещева».

2. Политика разработана с учетом требований Конституции Республики Беларусь, законодательных и иных нормативных правовых актов Республики Беларусь в области защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

3. Положения Политики служат основой для разработки локальных правовых актов, регламентирующих в учреждении образования «Пинский государственный аграрно-технический колледж имени А.Е.Клещева» (далее - Колледж) вопросы защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Колледжа, при этом первоочередной задачей является обеспечение безопасности всех активов Колледжа. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Колледжа. Главные цели Колледжа не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

5. 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.

ГЛАВА 2
ЦЕЛИ И ПРИЧИНЫ ЗАЩИТЫ ИНФОРМАЦИИ

6. Целями и причинами защиты информации являются:

6.1. сохранение конфиденциальности информационных ресурсов;

6.2. обеспечение непрерывности доступа к информационным ресурсам Колледжа для поддержки бизнес-деятельности;

6.3. защита целостности деловой информации с целью поддержания возможности Колледжа по оказанию услуг высокого качества и принятию эффективных управленческих решений.

ГЛАВА 3
НАЗНАЧЕНИЕ НАСТОЯЩЕЙ ПОЛИТИКИ

7. Повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Колледжа.

8. Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Колледже.

9. Обеспечение регулярного контроля за соблюдением положений настоящей Политики и проведение периодических проверок соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Колледжа.

ГЛАВА 4
ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ

10. Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Колледжа. 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.

11. Организации принадлежат на праве собственности (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.

ГЛАВА 5
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

12. В Колледжа используется информационная система, в которой обрабатываются персональные данные, за исключением специальных персональных данных, и которая не имеет подключений к открытым каналам передачи данных, отнесенная к соответствующему классу 4-ин типовых информационных систем.

ГЛАВА 6
СВЕДЕНИЯ О ПОДРАЗДЕЛЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ

13. В Колледже за защиту информации, ответственным за обеспечение защиты информации, в том числе и персональных данных, является инженер-программист.

14. Основными задачами инженера-программиста в области защиты информации являются:

14.1. разработка и внедрение организационных и технических мероприятий по комплексной защите информации Колледжа;

14.2. сохранение конфиденциальности документированной информации;

14.3. разработка проектов перспективных и текущих планов работ по комплексной защите информации Колледжа, составление отчетов об их выполнении;

14.4. разработка технических средств контроля по комплексной защите информации Колледжа;

14.5. формирование целей и задач работы по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации Колледжа;

14.6. обеспечение контроля за соблюдением нормативных требований по надежной защите информации;

14.7. обеспечение комплексного использования технических средств, методов и организационных мероприятий для защиты информации Колледжа.

ГЛАВА 7
ОБЩИЕ ПОЛОЖЕНИЯ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

15. Все работы в пределах Колледжа выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Колледже.

16. Внос в здания и помещения Колледжа личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т. п.), а также вынос их за пределы Колледжа производится только при согласовании с инженером-программистом.

17. Все данные (конфиденциальные или строго конфиденциальные), составляющие коммерческую тайну Колледжа и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Колледжа должны быть оснащены программным обеспечением по шифрованию жесткого диска. Инженер-программист периодически должен пересматривать права доступа сотрудников и других пользователей к соответствующим информационным ресурсам.

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

19. 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.

20. 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.

ГЛАВА 8
ДОСТУП ТРЕТЬИХ ЛИЦ К ИНФОРМАЦИОННЫМ СИСТЕМАМ ОРГАНИЗАЦИИ

21. Каждый сотрудник обязан немедленно уведомить инженера-программиста обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

22. 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.

ГЛАВА 9
УДАЛЕННЫЙ ДОСТУП

23. Пользователи получают право удаленного доступа к информационным ресурсам Колледжа с учетом их взаимоотношений с Колледжем.

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

25. Сотрудникам, работающим за пределами Колледжа с использованием компьютера, не принадлежащего Колледжа, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

26. 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.

27. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Колледжа, должны иметь программное обеспечение антивирусной защиты с последними обновлениями.

ГЛАВА 10
ДОСТУП К СЕТИ ИНТЕРНЕТ

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

29. Рекомендованные правила:

29.1. сотрудникам Колледжа разрешается использовать сеть Интернет только в служебных целях;

29.2. 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;

29.3. работа сотрудников Колледжа с интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Колледжа в сеть Интернет;

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

29.5. запрещен доступ в интернет через сеть Колледжа для всех лиц, не являющихся сотрудниками Колледжа, включая членов семьи сотрудников Колледжа.

30. Инженер-программист имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

ГЛАВА 11
ЗАЩИТА ОБОРУДОВАНИЯ

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

32. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит инженер-программист Колледжа.

ГЛАВА 12
АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

33. 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 компьютерным оборудованием.

Компьютерное оборудование, предоставленное Колледжу, является ее собственностью и предназначено для использования исключительно в производственных целях.

34. Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Колледжа, 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.

35. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т. д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

36. Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля.

37. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться в службу технической поддержки. 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.

38. При записи какой-либо информации на носитель для передачи его контрагентам и другим 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.

39. Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты, и прочие переносные устройства не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобных устройствах не рекомендуется хранить конфиденциальную информацию.

40. Порты передачи данных, в том числе FD и CD-дисководы, в стационарных компьютерах сотрудников Организации блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись информации у инженера-программиста Организации.

ГЛАВА 13
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

41. Все программное обеспечение, установленное на предоставленном Колледжу компьютерном оборудовании, является собственностью Колледжа и должно использоваться исключительно в производственных целях.

42. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, 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 Колледжа.

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

43.1. персональный межсетевой экран;

43.2. антивирусное программное обеспечение;

43.3. программное обеспечение шифрования жестких дисков;

43.4. программное обеспечение шифрования почтовых сообщений.

44. Все компьютеры, подключенные к сети Колледжа, должны быть оснащены системой антивирусной защиты, утвержденной инженером-программистом Организации.

45. Сотрудники Колледжа не должны:

45.1. блокировать антивирусное программное обеспечение;

45.2. устанавливать другое антивирусное программное обеспечение;

45.3. изменять настройки и конфигурацию антивирусного программного обеспечения.

46. Колледж предпочитает приобретать программное обеспечение, а не разрабатывать собственные программы, поэтому пользователям, желающим внедрить новые возможности бизнес-процессов, необходимо обсудить свое предложение с инженером-программистом Колледжа.

ГЛАВА 14
РЕКОМЕНДУЕМЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

47. Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами и другими для их использования в качестве доказательств в процессе судебного разбирательства и ином. Поэтому содержание электронных сообщений должно строго соответствовать стандартам Колледжа в области деловой этики.

48. Использование электронной почты в личных целях допускается в случаях, когда получение (отправка) сообщения не мешает работе других пользователей.

49. Сотрудникам запрещается направлять конфиденциальную информацию Колледжа по электронной почте без использования систем шифрования. Строго конфиденциальная информация Колледжа ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте.

50. Сотрудникам Колледжа запрещается использовать личные почтовые ящики электронной почты для осуществления деятельности Организации.

51. Использование сотрудниками Колледжа личных почтовых ящиков электронной почты осуществляется только при согласовании с инженером-программистом Колледжа при условии применения механизмов шифрования.

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

53. Сообщения, пересылаемые по электронной почте, имеют тот же статус, что и письма, и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

54. 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. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать инженера-програбммиста Колледжа.

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

56. Недопустимые действия и случаи использования электронной почты:

56.1. рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

56.2. групповая рассылка всем пользователям Колледжа сообщений/писем;

56.3. рассылка рекламных материалов, не связанных с деятельностью Колледжа;

56.4. подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

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

56.6. 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 Колледжа в области этики.

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

58. 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.

59. Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры Колледжа для других пользователей. Объем вложений не должен превышать 2 Мбайт.

ГЛАВА 15
СООБЩЕНИЯ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

60. 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.

61. В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте инженеру-программисту Колледжа.

62. Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

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

63.1. проинформировать инженера-программиста Колледжа;

63.2. не пользоваться и не выключать зараженный компьютер;

63.3. не подсоединять этот компьютер к компьютерной сети Колледжа до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование инженером-программистом Колледжа.

ГЛАВА 16
УПРАВЛЕНИЕ СЕТЬЮ

64. Инженер-программист Колледжа контролирует содержание всех потоков данных, проходящих через сеть Колледжа.

65. Сотрудникам Колледжа запрещается:

65.1. нарушать информационную безопасность и работу сети Колледжа;

65.2. сканировать систему безопасности;

65.3. контролировать работу сети с перехватом данных;

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

65.5. использовать любые программы, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя устройства;

65.6. передавать информацию о сотрудниках или списки сотрудников Колледжа посторонним лицам;

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

ГЛАВА 17
ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

66. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Инженер-программист Колледжа обязан оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

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

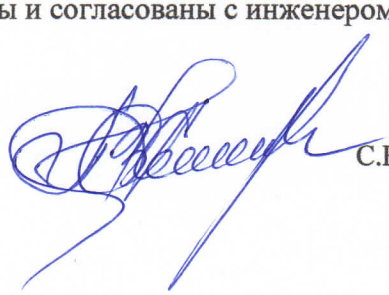
68. Только инженер-программист Колледжа на основании заявок руководителей структурных подразделений могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

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

70. Все заявки на проведение технического обслуживания компьютеров должны направляться инженеру-программисту Колледжа.

ГЛАВА 18
РАЗРАБОТКА СИСТЕМ И УПРАВЛЕНИЕ ВНЕСЕНИЕМ ИЗМЕНЕНИЙ

71. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и согласованы с инженером-программистом Колледжа.

Инженер – программист
учреждения образования «Пинский
государственный аграрно-технический
колледж имени А.Е.Клещева»  С.В. Пашкевич