УТВЕРЖДАЮ
Директор государственного
учреждения образования
«Солонская начальная школа
Жлобинского района»
_____Л.В.Таргонская

ПОЛИТИКА
информационной безопасности

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности в государственном учреждении образования «Солонская начальная школа Жлобинского района» (далее - Политика) определяет общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, в том числе и персональных данных.

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 государственном учреждении образования «Солонская начальная школа Жлобинского района» (далее – учреждение) вопросы защиты информации в информационных системах, предназначенных для обработки информации, распространение и предоставление которой ограничено.

4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник учреждения.

5. В настоящей Политике под термином «сотрудник» понимаются все сотрудники учреждения.

ГЛАВА 2
НАЗНАЧЕНИЕ НАСТОЯЩЕЙ ПОЛИТИКИ

6. Повышение осведомленности сотрудников в области рисков, связанных с информационными ресурсами учреждения.

7. Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в учреждении.

8. Обеспечение регулярного контроля за соблюдением положений настоящей Политики и проведение периодических проверок соблюдения информационной безопасности.

ГЛАВА 3
ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ

9. Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации учреждения. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных).

10. Учреждению 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 им деятельности в соответствии с действующим законодательством.

Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования учреждения образования, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала учреждения.

ГЛАВА 4
ОБЩИЕ ПОЛОЖЕНИЯ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

11. Все работы в пределах помещений учреждения выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в учреждении.

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

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

14. Сотрудники 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.

15. 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 5
ДОСТУП ТРЕТЬИХ ЛИЦ К ИНФОРМАЦИОННЫМ СИСТЕМАМ УПРАВЛЕНИЯ

16. Каждый сотрудник обязан немедленно уведомить руководство учреждения обо всех случаях предоставления доступа третьим лицам к ресурсам сети.

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

ГЛАВА 6
УДАЛЕННЫЙ ДОСТУП

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

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

20. Сотрудники, имеющие право удаленного доступа к информационным ресурсам учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети учреждения и к каким-либо другим сетям, не принадлежащим учреждению.

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

ГЛАВА 7
ДОСТУП К СЕТИ ИНТЕРНЕТ

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

23. Рекомендованные правила:

23.1. сотрудникам учреждения разрешается использовать сеть Интернет только в служебных целях;

23.2. 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;

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

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

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

ГЛАВА 8
ЗАЩИТА ОБОРУДОВАНИЯ

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

25. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

ГЛАВА 9
АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

26. 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 (перечень информационных ресурсов прилагается).

Компьютерное оборудование, предоставленное учреждением, является его собственностью и предназначено для использования исключительно в служебных целях.

27. Пользователи портативных компьютеров, содержащих информацию учреждения, 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.

ГЛАВА 10
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

28. Все программное обеспечение, установленное на предоставленном учреждением компьютерном оборудовании, является

собственностью учреждения и должно использоваться исключительно в служебных целях.

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

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

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

32. Сотрудники учреждения не должны:

32.1. блокировать антивирусное программное обеспечение;

32.2. устанавливать другое антивирусное программное обеспечение;

32.3. изменять настройки и конфигурацию антивирусного программного обеспечения.

ГЛАВА 11
РЕКОМЕНДУЕМЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

33. Содержание электронных сообщений (удаленные или не удаленные) должно строго соответствовать стандартам учреждения в области деловой этики.

34. Строго конфиденциальная информация учреждения ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте.

35. Сотрудникам учреждения запрещается использовать личные почтовые ящики электронной почты для осуществления деятельности учреждения образования.

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

37. В целях предотвращения ошибок при отправке сообщений сотрудники перед отправкой должны внимательно проверить правильность написания имен и адресов получателей.

38. Недопустимые действия и случаи использования электронной почты:

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

38.2. 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 учреждения образования в области этики.

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

40. 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 учреждении образования процедурами документооборота.

ГЛАВА 12
СООБЩЕНИЯ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

41. Все сотрудники должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности.

42. В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте руководству учреждения образования.

43. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан проинформировать руководство учреждения для принятия мер по защите информации.

ГЛАВА 13
ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

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

45. Необходимо регулярно делать резервные копии всех основных служебных данных.

46. 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.

ГЛАВА 14
ВОЗЛОЖЕНИЕ ОБЯЗАННОСТЕЙ ПО ОБЕСПЕЧЕНИЮ КОНТРОЛЯ

47. Возложить обязанности по обеспечению контроля за ее соблюдением на учителя, обладающего соответствующими знаниями и опытом профессиональной деятельности.

48. Ответственному специалисту предоставлять докладные записки на имя руководителя по каждому установленному факту нарушения политики безопасности, с последующим проведением по ним служебных разбирательств и принятием необходимых мер реагирования.

49. Меры ответственности за факты нарушения политики информационной безопасности несут, как со стороны ответственных лиц, так и иных работников предприятия.

50. Исключить возможность использования сторонних МНИ (флешки, жесткие диски и т.д.) на рабочих местах без предварительной проверки содержимого на предмет вредоносного ПО лицами, ответственными за соблюдение политики безопасности.

51. Разграничить доступ пользователей при работе на ПЭВМ (создание персональных учетных записей с соблюдением требований политики безопасности паролей).

52. Запреть хранение паролей к учетным записям пользователей в текстовых или иных файлах на локальных дисках.

53. Своевременно и регулярно создавать резервные копии файлов системы (back-up) и сохранять на отдельных серверах или в облачных хранилищах данных.

54. Протоколировать и документировать (ведение log-файлов) действий всех файлов.

55. Осуществлять настройки сетевого оборудования при необходимости использования удаленного доступа исключительно выделенным кругом лиц с указанием конкретных IP или MAC-адресов рабочих станций.

56. Обязательно изменять заводские реквизиты доступа (логин и пароль) вновь приобретаемого и монтируемого сетевого оборудования.

57. Использовать исключительно лицензионные антивирусные программные продукты на рабочих станциях и серверах.

ГЛАВА 15
ОТВЕТСТВЕННОСТЬ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

58. Ответственность за соблюдение информационной безопасности несет каждый сотрудник учреждения образования при работе с информационными активами в пределах его полномочий.

59. Меры ответственности за факты нарушения политики безопасности как со стороны ответственных лиц, так и иных работников предприятия, организации:

Преступления против информационной безопасности

Хищение путем использования компьютерной техники (ст.212 УК РБ)

Ответственность за деяния, предусмотренные ст.212, наступает с 14- летнего возраста.

59.1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации

- ***наказывается лишением свободы до трех лет.***

59.2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации

- ***наказывается лишением свободы от двух до пяти лет.***

59.3. Деяния, предусмотренные частями 1 или 2 настоящей статьи, совершенные в крупном размере,

- ***наказываются лишением свободы на срок от двух до семи лет со штрафом или без штрафа и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.***

59.4. Деяния, предусмотренные частями 1, 2 или 3 настоящей статьи, совершенные организованной группой либо в особо крупном размере

- ***наказываются лишением свободы на срок от пяти до двенадцати лет.***

Несанкционированный доступ к компьютерной информации (ст. 349 УК РБ)

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда

- **наказывается штрафом или арестом на срок до шести месяцев.**

Модификация компьютерной информации (ст. 350 УК РБ)

Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности

- ***наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.***

Компьютерный саботаж (ст. 351 УК РБ)

Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж)

- ***наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом***

на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

Неправомерное завладение компьютерной информацией (ст.352 УК РБ)

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда

- ***наказываются общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.***

Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353 УК РБ)

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети

-наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.

Разработка, использование либо распространение вредоносных программ(ст. 354 УК РБ)

Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами

- ***наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.***

Нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК РБ)

Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда,

- ***наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или***

исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.