МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«Центр детского творчества»
Ленинского района г. Саратова

Политика информационной безопасности
МУ ДО «ЦДТ» Ленинского района г. Саратова

1. Общие положения

1.1. Политика информационной безопасности Муниципального учреждения дополнительного образования «Центр детского творчества» Ленинского района г. Саратова (далее – Центр) 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 Центра при осуществлении своей деятельности.
1.2. Основной целью Политики информационной безопасности Центра является защита информации Центра 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.
1.3. Политика информационной безопасности разработана в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи», Указом президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением правительства РФ № 781 от 17 ноября 2007 года «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением правительства РФ № 687 от 15 сентября 2008 года «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.
1.4. Выполнение требований Политики ИБ является обязательным для всех структурных подразделений Центра.
1.5. Ответственность за соблюдение информационной безопасности несет каждый сотрудник учреждения. На лиц, работающих в управлении по договорам гражданско-правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

2. Цель и задачи политики информационной безопасности

2.1. Основными целями политики ИБ являются:
- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам учреждения;
- защита целостности информации с целью поддержания возможности учреждения

по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами учреждения;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
- предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2. 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 учреждения;
- выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ учреждения;
- организация антивирусной защиты информационных ресурсов учреждения;
- защита информации учреждения от несанкционированного доступа (далее – НСД) и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору Центра.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ Центра 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 учреждения, 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.

3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал Центра. 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.

3.3. Стратегия обеспечения ИБ Центра 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 Центра.

4. Основные принципы обеспечения информационной безопасности

4.1.Основными принципами обеспечения ИБ:
- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов Центра;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ Центра, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;

- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками Центра за обеспечение ИБ учреждения исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты

5.1. Объектами защиты с точки зрения ИБ в управлении являются:
- информационный процесс профессиональной деятельности;
- информационные активы Центра.

5.2. Защищаемая информация делится на следующие виды:
- информация по финансово-экономической деятельности Центра;
- 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

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

6.2. Внос в здание и 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 администрацией Центра.

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

6.4. Каждый сотрудник обязан немедленно уведомить администрацию Центра обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

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

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

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

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

Рекомендованные правила:
- сотрудникам Центра 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;
- сотрудники Центра не должны использовать сеть Интернет для хранения корпоративных данных;
- сотрудники Центра перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Центра для всех лиц, не являющихся сотрудниками Центра, включая членов семьи сотрудников учреждения.

6.7. Администрация Центра 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 Центра.

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

6.9. 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 Центром, является его собственностью и предназначено для использования исключительно в производственных целях.

6.10. Каждый сотрудник, получивший в пользование компьютерное оборудование, обязан принять надлежащие меры по обеспечению его сохранности.

6.11. Все компьютеры должны защищаться паролем при загрузке системы. 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.

6.20. 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.

6.21. Все программное обеспечение, установленное на предоставленном Центром компьютерном оборудовании, является собственностью Центра и должно использоваться исключительно в производственных целях.

6.22. 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 Центра.

6.23. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной администрацией Центра.

6.24. Сотрудники Центра не должны:
- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.25. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Строго конфиденциальная информация учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

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

6.27. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронныхкоммуникаций, имеющих тот же статус, что 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.

6.28. 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.

6.29. 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.

6.30. В случае кражи переносного компьютера следует незамедлительно сообщить администрации Центра.

6.31. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
- проинформировать администрацию Центра;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Центра до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное

сканирование.

6.35. Сотрудникам учреждения запрещается:

- нарушать информационную безопасность и работу сети Центра;
- сканировать порты или систему безопасности;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или списки сотрудников учреждения посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

6.38. 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.

6.39. Все заявки на проведение технического обслуживания компьютеров должны направляться администрации Центра.

7. Управление информационной безопасностью

7.1 Управление ИБ Центра 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;
- осуществление контроля (мониторинга) функционирования системы.

8. Реализация политики информационной безопасности

8.1.Реализация Политики ИБ Центра осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности.

9. Порядок внесения изменений и дополнений в политикуинформационной безопасности

9.1.Внесение изменений и дополнений в Политику информационной безопасности производится 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

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности Центра возлагается на администрацию Центра.