УТВЕРЖДАЮ:
Исп. директор МАУ ДО ДЮЦ «Каскад»
_____ В.А.Трынкина
_____ 2017г.

Политика информационной безопасности
муниципального автономного учреждения дополнительного образования
«Детско-юношеский Центр «Каскад»

1. Общие положения.

1.1. Политика информационной безопасности МАУ ДО ДЮЦ «Каскад» (далее – Учреждение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми руководствуются работники Учреждения при осуществлении своей деятельности.

1.2. Политика информационной безопасности разработана в соответствии с Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ № 687 от 15.09.08г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. Выполнение требований Политики информационной безопасности является обязательным для всех участников образовательного процесса.

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

1.5. Внесение изменений и дополнений в Политику информационной безопасности производится по мере необходимости, но 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.

2. Цель и задачи политики информационной безопасности.

2.1. Основной целью политики информационной безопасности Учреждения является защита его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования Учреждения.

Задачи Политики информационной безопасности:

- сохранение конфиденциальности 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;

- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;

- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности Учреждения.

3. Стратегия и направления обеспечения информационной безопасности.

3.1. Стратегия обеспечения Политики информационной безопасности заключается в использовании программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников Учреждения и противодействовать иным внешним и внутренним угрозам.

3.2. Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

- утрата сведений, составляющих защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;
- утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также несанкционированное копирование или хищение информации по каналам связи;
- недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем, серверов, маршрутизаторов, систем управления баз данных, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств.

3.3. 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.

3.4. Основными направлениями обеспечения информационной безопасности являются:

- обеспечение информационной безопасности при ведении делопроизводства и осуществлении документооборота (при использовании средств автоматизации, а также без использования средств автоматизации);

- обеспечение информационной безопасности при осуществлении взаимодействий с другими организациями;

- обеспечение информационной безопасности при соблюдении договорных требований;

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

- своевременное обнаружение и устранение рисков, потенциально способных повлиять на информационную безопасность Учреждения;

- разработка и внедрение защитных мер, в том числе обеспечение антивирусной защиты;

- контроль эффективности принимаемых защитных мер;

- разделение зон ответственности между сотрудниками Учреждения за обеспечение информационной безопасности исходя из принципа персональной и единоличной ответственности за совершаемые операции;

- повышение знаний и квалификации сотрудников Учреждения в вопросах обеспечения информационной безопасности;

- разработка локальных нормативных документов по обеспечению информационной безопасности в Учреждении;

- создание условий для доступа сотрудников Учреждения только к тем Интернет-ресурсам, содержание которых не противоречит законодательству Российской Федерации и не является несовместимым с целями и задачами обучения и воспитания обучающихся.

4. Объекты защиты.

Объектами защиты, которые необходимо защищать с точки зрения информационной безопасности, являются:

- информация,
- носитель информации,
- информационный процесс,
- помещения, в которых расположены средства обработки защищаемой информации.

5. Требования по информационной безопасности

5.1. Информация является важным активом Учреждения и ее защита является обязанностью каждого сотрудника.

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

5.3. Все конфиденциальные данные, хранящиеся на жестких дисках компьютеров Учреждения, должны быть защищены паролем (закодированы).

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

5.5. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности, посещения сайтов, содержащих призывы к насилию и насильственному изменению основ конституционного строя, разжигающие социальную, расовую, межнациональную и религиозную рознь, пропаганду наркомании, экстремистских религиозных и политических идей, информацию сексуального характера,

5.6. Сотрудники Учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов.

5.7. Доступ в Интернет через сеть Учреждения запрещен для всех лиц, не являющихся сотрудниками Учреждения, включая членов семьи сотрудников.

5.8. Не допускается использование электронной почты Учреждения в личных целях. Сотрудники Учреждения для обмена документами и информацией должны использовать только свой официальный адрес электронной почты.

5.9. Запрещается пересылка с использованием электронной почты Учреждения любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим 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.

5.10. Все программное обеспечение, установленное на компьютерном оборудовании Учреждения, является собственностью Учреждения и должно использоваться исключительно в производственных целях.

5.11. Перед утилизацией все компоненты компьютерного оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверить на предмет отсутствия на них конфиденциальных данных и выполнить процедуру форматирования носителей информации, исключающую возможность восстановления данных.

5.12. Все пользователи должны сообщать администрации Учреждения об известных или подозреваемых ими нарушениях информационной безопасности в Учреждении.

5.13. В случае выявления наличия вирусов запрещается включать и использовать зараженный компьютер, пока в нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.

5.14. Аудио-, видеозапись, фотографирование во время совещаний, заседаний, собраний можно вести только после получения разрешения руководителя Учреждения или председателя собрания.
5.15. Сотрудникам Учреждения запрещается:
- нарушать информационную безопасность и работу Интернет-сети Учреждения;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или обучающихся посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение;
- устанавливать на компьютерном оборудовании Учреждения нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности;
- блокировать антивирусное программное обеспечение, самостоятельно изменять конфигурацию программного обеспечения.
5.16. Ответственность за сохранность данных на стационарных и портативных компьютерах лежит на пользователях.
5.17. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.
5.18. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть согласованны с администрацией Учреждения.
5.19. Все заявки на проведение технического обслуживания компьютеров должны направляться заместителю директора по АХЧ.
5.20. В связи с отсутствием в штате Учреждения IT-специалиста, программиста, Отдела информационной безопасности, обслуживание офисной техники (в том числе компьютеров) ведется сторонними организациями путем заключения договора, на условиях выполнения все требования Российского законодательства в области защиты информации.

6. Управление информационной безопасностью.
6.1. Управление информационной безопасностью Учреждения включает в себя:
- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- осуществление контроля (мониторинга) функционирования системы информационной безопасности;
- оценку рисков, связанных с нарушениями Политики информационной безопасности.
6.2. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности Учреждения возлагается на сотрудника, назначенного приказом директора Учреждения.