Согласовано на заседании педагогического совета МБУ ДО ЦДНТТ протокол №2 от «30» 10 2018 г.	Утверждаю Директор МБУ ДО ЦДНТТ Е.А. Андросова Приказ № 102-ОД от «2» 11 2018 г.

Политика информационной безопасности МБУ ДО ЦДНТТ МО «Намский улус» РС (Я).

1. Общие положения

1.1.Политика информационной безопасности МБУ ДО ЦДНТТ 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 учреждения при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности является защита информации учреждения 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 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным закон 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 РФ №781 от 17.11.07г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ №687 от 15.09.08г. «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 работник учреждения.

1.5.Ответственность за соблюдение информационной безопасности несет каждый работник учреждения. На лиц, работающих 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 работников по обеспечению информационной безопасности. -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 учреждения.

3. Концептуальная схема обеспечения информационной безопасности

3.1.Политика ИБ учреждения направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий работников 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 учреждения. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией работников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.
3.3.Стратегия обеспечения ИБ учреждения 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 работников учреждения.

4. Основные принципы обеспечения информационной безопасности

4.1.Основными принципами обеспечения ИБ являются:
-постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов учреждения;
-своевременное обнаружение проблем, потенциально способных повлиять на ИБ учреждения, корректировка моделей угроз и нарушителя;
-разработка и внедрение защитных мер;
-контроль эффективности принимаемых защитных мер;
-персонификация и разделение ролей и ответственности между работниками учреждения 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 школы.
5.2.Защищаемая информация делится на следующие виды:
- информация по финансово-экономической деятельности школы;
- 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.В отношении всех собственных информационных активов учреждения, активов, находящихся под контролем учреждения, а также активов, используемых для получения доступа к инфраструктуре учреждения, должна быть определена ответственность соответствующего работника учреждения. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами учреждения должна доводиться до сведения директора учреждения.
6.2. Все работы в пределах учреждения должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.
6.3.Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну учреждения и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. При этом на персональных компьютерах педагогов, на которых не размещена информация, содержащая персональные данные или гриф «Для служебного пользования»/«Конфиденциально» устанавливать пароли запрещено.
6.4.Системный администратор должен периодически пересматривать права доступа работников и других пользователей к соответствующим информационным ресурсам.
6.5.В целях обеспечения санкционированного доступа к информационному конфиденциальному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.
6.6.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.
6.7. В процессе работы с информацией, требующей информационной защиты, работники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.
6.8. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности. Рекомендованные правила:
- работникам учреждения 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;

- работа работников учреждения с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации учреждения в сеть Интернет;
- работникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем учреждения;
- работники учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть учреждения для всех лиц, не являющихся работниками учреждения, включая членов семьи работников.

6.9.Администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.10. работники изменения производит администратор ЛВС.

6.12.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 учреждением, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

6.14. 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.

6.15.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.

6.16.Порты передачи данных, в том числе CD дисководы в стационарных компьютерах работников учреждения блокируются, за исключением тех случаев, когда работником получено разрешение на запись от администратора.

6.17.Все программное обеспечение, установленное на предоставленном учреждением компьютерном оборудовании, является собственностью учреждения и должно использоваться исключительно в производственных целях.

6.18.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 учреждения.

6.19.На всех портативных компьютерах, содержащих информацию, требующую защиты, должны быть установлены программы, необходимые для обеспечения защиты информации:
- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков.

6.20.Работники учреждения не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.
6.21.Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Работникам запрещается направлять конфиденциальную информацию учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация учреждения ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте.
6.22.Использование работниками учреждения публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.
6.23.Сотрудники учреждения для обмена документами должны использовать только свой официальный адрес электронной почты.
6.24.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. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.
6.25.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.
6.26.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.
6.27.В случае кражи переносного компьютера следует незамедлительно сообщить администратору и/или директору учреждения.
6.28.Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
-проинформировать администратора;
- не использовать и не включать зараженный компьютер;
-не подсоединять этот компьютер к компьютерной сети учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.
6.29.Перечень помещений с техническими средствами информационной безопасности утверждается директором учреждения.
6.30. Работникам учреждения запрещается:

- нарушать информационную безопасность и работу сети учреждения;
- 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;
- передавать информацию о работниках или списки работников учреждения посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

6.33.Все заявки на проведение технического обслуживания компьютеров должны направляться администратору.

6.34.Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованны с администратором.

7.Управление информационной безопасностью

7.1.Управление ИБ учреждения 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 ИБ;

-оценку рисков, связанных с нарушениями ИБ.

8. Реализация политики информационной безопасности

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

9.Порядок внесения изменений и дополнений в политику информационной безопасности

9.1.Внесение изменений и дополнений в Политику информационной безопасности производится 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.

10.Контроль за соблюдением политики информационной безопасности

10.1.Текущий контроль за соблюдением выполнения требований Политики информационной безопасности учреждения возлагается на работника, назначенного приказом директора учреждения.

10.2.Директор учреждения на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.