Политика информационной безопасности МБОУ «Намской начальной школы – детский сад»

1. Общие положении

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности.

Настоящая Политика информационной безопасности (Далее – Политика ИБ) разработана в соответствии с Трудовым кодексом Российской Федерации от 30.12.2001 г. № 197-ФЗ (с изм. и доп.), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральным законом от 29.12. 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»; Федеральным законом от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»; Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи»; Распоряжением Правительства Российской Федерации от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей»; Постановлением Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановлением Правительства Российской Федерации от 10.07.2013 г. №582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации»; Постановлением Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Федеральным законом от 29.12.2012 N 273-ФЗ (ред. от 29.07.2017) «Об образовании в Российской Федерации»; Указом Президента Республики Саха (Якутия) от 22.12.2004 г. № 1900 «О Концепции информационной безопасности Республики Саха (Якутия)»; Приказом Рособрнадзора от 29 мая 2014 г. № 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации» (с изменениями и дополнениями);Приказом Федеральной службы по техническому и экспортному (ФСТЭК) от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; Приказом Министерства финансов Российской Федерации от 21.07.2011г. № 86н «Об утверждении порядка предоставления информации государственным (муниципальным) учреждением, её размещения на официальном сайте в сети Интернет и ведения указанного сайта»;

Правилами подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации(утв. Минобрнауки России 11.05.2011 N АФ-12/07вн); Письмом Минобрнауки России от 28.04.2014 N ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании

ресурсов сети «Интернет» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования», «Рекомендациями по организации системы ограничения в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»);
Приказом МКУ «Управление образования МО «Намский улус» РС(Я)» от 31.10.2017 г.№ 01-08/990 «О введении в действие политики оператора в отношении обработки персональных данных» и иными федеральными законами и нормативно-правовыми актами.
1.2. Под информационной безопасностью организации следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.
Система информационной безопасности (Далее - СИБ) направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.
1.3. К объектам информационной безопасности в организации относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами Российской Федерации, в т. ч. персональные данные;
- средства и системы информатизации. программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.4. СИБ должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата):
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.6 Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба;
- издание нормативных и распорядительных документов, определяющих порядок выделения сведений конфиденциального характера и механизмы их защиты;
- право включать требования по обеспечению информационной безопасности в коллективный договор;
- право включать требования по защите информации в договоры по всем видам деятельности;
- разработка перечня сведений конфиденциального характера;
- право требовать защиты интересов образовательной организации со стороны государственных и судебных инстанций.

2. Правовые нормы обеспечения информационной безопасности

2.1. Образовательная организация имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся,

работников образовательной организации, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. Образовательная организация обязана обеспечить сохранность конфиденциальной информации.

2.3. Руководство образовательной организации:

- назначает ответственного за обеспечение информационной безопасности.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ руководителя образовательной организации о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников образовательной организации и др.

2.5. порядок допуска сотрудников образовательной организации к информации предусматривает:

- принятие работниками обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работников с нормами законодательства Российской Федерации, Республики Саха (Якутия), местного самоуправления и образовательной организации об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работников ответственным по информационной безопасности;
- контроль работников ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности

3.1. Для обеспечения информационной безопасности в образовательной организации требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности образовательной организации;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся образовательной организации;
- учет всех носителей конфиденциальной информации.

3.2. Использование сети Интернет работниками образовательной организации допускается только в целях исполнения ими своих должностных обязанностей и в целях образовательного процесса, использование сети Интернет обучающимися допускается только для обеспечения образовательного процесса.

3.3. Использование сети Интернет в образовательной организации в личных целях работниками и обучающимися не допускается.

3.4. В целях своевременного выявления угроз, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, в образовательной организации проводится периодический контроль состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет, в том числе контроль функционирования технических средств контентной фильтрации и антивирусной защиты.

Периодичность такого контроля и состав мероприятий по контролю устанавливается руководителем образовательной организации.

3.5. Обучающиеся в случае выявления наличия доступа к ресурсам сети Интернет,

содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, незамедлительно информирует педагогического работника, ведущего занятие, или иного ответственного работника образовательной организации.

3.6. Педагогический работник, ведущий занятие, иной ответственный работник образовательной организации обязан осуществлять постоянный контроль использования технических средств, применяемых при организации доступа к сети Интернет (программных, программно-аппаратных), в том числе контроль функционирования технических средств контентной фильтрации, а также контроль доступа обучающихся к ресурсам сети Интернет.

При получении информации от обучающихся о получении доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, или в случае самостоятельного выявления наличия доступа к таким ресурсам сети Интернет, незамедлительно принимать меры, направленные на прекращение и ограничение доступа обучающихся к такой информации, а также информировать об инциденте работника образовательной организации, ответственного за организацию доступа к сети Интернет.

3.7. При организации доступа и использовании сети Интернет в образовательной организации работники образовательной организации несут персональную ответственность в соответствии действующим законодательством Российской Федерации.

3.8. Обучающиеся и их родители (законные представители) несут ответственность за неправомерное использование сети Интернет в порядке, установленном в образовательной организации, и в соответствии с действующим законодательством Российской Федерации.

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

3.10. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики ИБ являются собственностью организации.

3.11. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки».

Для установки режимов защиты пользователь должен обратиться к администратору сети. 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.

3.12. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация образовательной организации.

3.13. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор локальной вычислительной сети (ЛВС).

3.14. Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору. Локальное техническое обслуживание должно осуществляться только при личном присутствии пользователя. Дистанционное техническое

обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест (Далее - АРМ), конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться. При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений. Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации, в том числе в составе АРМ допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ. Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем. АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками организации. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной системы организации. При передаче указанного АРМ другому пользователю по другой должности, должна производиться гарантированная очистка диска (форматирование). Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

4. Организация работы с документами и информационными ресурсами, технологиями

4.1. Составные части делопроизводства:

- бумажное делопроизводство;
- электронное делопроизводство;
- системы взаимодействия и сопряжения бумажного и электронного делопроизводства.

4.2. Система организации делопроизводства:

- учет документов образовательной организации, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет входящих (исходящих) документов образовательной организации в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- исключение необоснованного ознакомления с документами лиц, не имеющих нужных полномочий;
- уничтожение документов.

4.2. В ходе использования, передачи, копирования и исполнения документов необходимо соблюдать определенные правила:

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

4.2.2. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

4.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

4.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

4.2.5. Запрещается выносить документы с грифом «Для служебного пользования» за

пределы образовательной организации.
4.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.
4.3.Для организации делопроизводства приказом руководителя образовательной организации назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной руководителем образовательной организации. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. Обеспечение безопасности в Автоматизированной информационной системе

5.1. Автоматизированная информационная система(Далее - АИС) относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.
АИС обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.
Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой АИС.
5.2. Сотрудники, получившие доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными положениями организации, (согласно занимаемой должности), а именно с инструкциями по обращению с носителями конфиденциальной информации. Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставляет только администратор информационной системы.
Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.
5.3. Регламент общих ограничений для участников образовательного процесса при работе с АИС, обеспечивающей предоставление услуги.
5.3.1. Участники образовательного процесса, имеющие доступ к АИС, не имеют права передавать персональные права доступа (логины и пароли) для входа в АИС другим лицам. Передача персональных прав доступа для входа в Автоматизированную информационную систему другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.
5.3.2. Участники образовательного процесса, имеющие доступ к АИС, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).
5.3.3. Участники образовательного процесса, имеющие доступ к АИС, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя образовательной организации, службу технической поддержки АИС.
5.3.4. Все операции, произведенные участниками образовательного процесса, имеющими доступ к АИС, с момента получения информации руководителем образовательной организации и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.

5.3.5. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться. Предпочтительно использовать механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие информационные системы. При невозможности автоматического блокирования учетных записей, сотрудникам сопоставляются временные учетные записи (с фиксированным сроком действия), о чем делается отметка в заявке при ее исполнении и в обязательном порядке доводится до инициатора заявки. При проведении работ по обеспечению безопасности информации в АИС участники образовательного процесса, имеющие доступ к АИС, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

6. Ведение и сопровождение официального сайта

6.1. Информационный ресурс сайта образовательной организации формируется в соответствии с деятельностью всех структурных подразделений образовательной организации, педагогических работников, обучающихся, их родителей (законных представителей), деловых партнеров и прочих заинтересованных лиц.

6.2. Информационный ресурс сайта образовательной организации является открытым и общедоступным.

6.3. Условия размещения ресурсов ограниченного доступа регулируются отдельными документами. Размещение таких ресурсов допустимо только при наличии соответствующих организационных и программно-технических возможностей, обеспечивающих защиту персональных данных и авторских прав.

6.4. На сайте образовательной организации размещается обязательная информация согласно приказу Рособрнадзора от 29 мая 2014 г. № 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации» (с изменениями и дополнениями).

6.5. На сайте образовательной организации могут быть размещены другие информационные ресурсы: общая информация об образовательном учреждении; история образовательного учреждения; материалы о научно-исследовательской деятельности обучающихся, воспитанников и их участии в олимпиадах и конкурсах; электронные каталоги информационных ресурсов образовательной организации; материалы о руководителях, педагогах, выпускниках, деловых партнерах образовательной организации с переходом на их сайты, блоги; фотоматериалы, форум; гостевая книга.

6.6. Часть информационного ресурса, формируемого по инициативе подразделений (методических объединений, детских организаций, музеев), творческих коллективов, педагогов и обучающихся, воспитанников образовательного учреждения, может быть размещена на отдельных специализированных сайтах, доступ к которым организуется с сайта образовательной организации, при этом данные сайты считаются неотъемлемой частью сайта образовательной организации и на них распространяются все нормы и правила действующего положения о сайте образовательной организации.

6.7. Не допускается размещение на сайте образовательной организации противоправной информации и информации, не имеющей отношения к деятельности образовательной организации, несовместимой с задачами образования, разжигающей межнациональную рознь, призывающей к насилию, не подлежащей свободному распространению в соответствии с законодательством Российской Федерации.

6.8. Ответственность за нарушение работоспособности и актуализации сайта образовательной организации вследствие реализованных некачественных концептуальных решений, отсутствия чёткого порядка в работе лиц, на которых возложено предоставление информации, несёт ответственный за информатизацию образовательного процесса.

7. Работа с криптографическими системами

7.1. К работе с криптографическими системами допускаются только сотрудники, имеющие соответствующее разрешение от руководства организации.

7.2. Секретные ключи электронно-цифровых подписей и шифрования должны храниться в сейфах под ответственностью лиц на то уполномоченных. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования должен быть исключен.

7.3. Категорически запрещается:

- выводить секретные ключи и шифрования на дисплей компьютера или принтер;
- записывать на носитель секретных ключей и шифрования постороннюю информацию.

7.4. При компрометации секретных ключей, шифрования и прочей электронной информации и информационных технологий принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и шифрования, паролей. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения руководства организации.

8. Заключительные положения

8.1.1. Требования настоящей Политики ИБ могут развиваться другим внутренними нормативными документами организации, которые дополняют и уточняют ее. В случае изменения действующего законодательства и иных нормативных актов, а также устава организации настоящая Политика ИБ и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также уставу организации.