Утверждаю
Руководитель КГКП «Ясли-сад «Шапағат» отдела образования Костанайского района» Управления образования акимата Костанайской области
_____ Алпысбаева Г.Б

Политика информационной безопасности

КГКП «Ясли-сад «Шапағат» отдела образования Костанайского района» Управления образования акимата Костанайской области

1. Общие положения

1.1. Политика информационной безопасности КГКП «Ясли-сад «Шапағат» отдела образования Костанайского района» Управления образования акимата Костанайской области (далее – организация образования), 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 организации образования при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности организации образования является защита информации организации образования при осуществлении образовательной 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 Законом Республики Казахстан от 6 января 2012 года ЛФ 527-IV « О национальной безопасности», Законом Республики Казахстан от 24 ноября 2015 года ЛГУ 418-V «Об информатизации», Законом Республики Казахстан от 15 марта 1999 года N2 349-1 «О государственных секретах», Законом Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите», Законом Республики Казахстан от 7 января 2003 года N9 370 «Об электронном документе и электронной цифровой подписи», Законом Республики Казахстан от 5 июля 2004 года № 567-11 «О связи», Постановлением Правительства Республики Казахстан от 20 декабря 2016 года 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной

безопасности», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4Ответственность за соблюдение информационной безопасности несет каждый сотрудник организации образования.

2. Цель и задачи политики информационной безопасности

2.1. Основными целями политики ИБ являются:

-сохранение конфиденциальности критичных информационных ресурсов; -защита целостности информации с целью поддержания возможности отдела 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 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 отдела;

-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ отдела;

-организация антивирусной защиты информационных ресурсов отдела организации образования;

защита информации организации образования 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 организации образования .

3. Концептуальная схема обеспечения информационной безопасности

3.1.Политика ИБ отдела 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 организации образования , 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 организации образования . 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 внештатной ситуации.

3.3. Стратегия обеспечения ИБ отдела заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от техник.

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 организации образования;

-своевременное обнаружение проблем, потенциально способных повлиять на ИБ организации образования, корректировка моделей угроз и, нарушителя;

-разработка и внедрение защитных мер;

-контроль эффективности принимаемых защитных мер;

-персонификация и разделение ролей и ответственности между сотрудниками организации образования за обеспечение ИБ организации образования 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 организации образования.

5.2. Защищаемая информация делится на следующие виды:

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 организации образования , активов, находящихся под контролем организации образования, а также активов, используемых для получения доступа к инфраструктуре организации образования, должна быть определена ответственность соответствующего сотрудника организации образования. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами организации образования должна доводиться до сведения руководителя организации образования.

6.2. Все работы в пределах организации образования должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

6.3. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну организации образования и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

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

6.5. 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.

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

6.7. Рекомендованные правила:

- сотрудникам организации образования 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 сотрудников отдела с интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации организации образования в сеть ,

-сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем организации образования ;

-сотрудники отдела перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирус - запрещено использование сторонних почтовых служб (зарубежных служб @mail.ru, @gmail.com и т.д.) в служебной деятельности. В работе разрешается использовать почтовые службы такие как mail.kz, post.kz, nur.kz;

- запрещена передача служебной информации без пометки, с пометкой ДСП, с грифом «секретно» по средствам мессенджеров WhatsApp, Telegram, Viber, Vk.com, Facebook и другие;

запрещена фото и видеосъемка проектов документов, а также самих документов (без пометки, с пометкой ДСП, с грифом);

- запрещено подключение смартфонов к рабочим компьютерам для зарядки, передачи файлов, фото и другое;
- запрещено использование программ удалённого доступа (TeamViewer, Radmin, AnyDesk, Supremo и т.д.;
- запрещен доступ в Интернет через сеть колледжа для всех лиц, не являющихся сотрудниками отдела, включая членов семьи сотрудников. 6.8. Администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

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

6.10. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит инженер по ПО или лицо его заменяющее.

6.11. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CT)-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование" Компьютерное оборудование, предоставленное отделом, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

6.13. Все компьютеры могут быть защищены паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки» . 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 формирования носителей информации, исключающая возможность восстановления данных.

6.14. 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.

6.15. Порты передачи данных, в том числе СД дисководы в стационарных компьютерах сотрудников организации образования блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

6.16. Все программное обеспечение, установленное на предоставленном организации образования компьютерном оборудовании, является собственностью организации образования и должно использоваться исключительно в производственных целях.

6.17. 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 непосредственно руководителю организации образования .

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

- персональный межсетевой экран;
- антивирусное программное обеспечение;

6.19. Сотрудники организации образования не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.20. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается.

Конфиденциальная информация организации образования, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.21. Использование сотрудниками организации образования публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации.

6.22. Сотрудники организации образования для обмена документами должны использовать только свой официальный адрес электронной почты.

6.23. 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.

6.25. 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.

6.26. В случае кражи переносного компьютера следует незамедлительно сообщить администратору или руководителю организации образования .

6.27. Если имеется подозрение или выявлено наличие вирусов разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

-проинформировать инженера по ПО или лицо его заменяющее;

- не использовать и не включать зараженный компьютер;

-не подсоединять этот компьютер к компьютерной сети организации образования до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование инженером по ПО или лицом его заменяющим.

6.28. Сотрудникам организации образования запрещается:

- нарушать информационную безопасность и работу сети организации образования ;
- 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 сотрудниках или списки сотрудников отдела посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

6.31. Все заявки на проведение технического обслуживания компьютеров должны направляться инженеру по ПО или лицу его заменяющему.

7. Управление информационной безопасностью

7.1. Управление ИБ организации образования 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 отдела 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 организации образования возлагается на заместителя руководителя организации образования (т.е на методиста организации образования)