Утверждена
решением Правления АОО
«Назарбаев Интеллектуальные школы»
от 14 сентября 2017 года
(протокол № 47)

Политика информационной безопасности

автономной организации образования «Назарбаев Интеллектуальные школы», ее филиалов и дочерних организаций

1. Общие положения

1.Настоящая Политика информационной безопасности автономной организации образования «Назарбаев Интеллектуальные школы», ее филиалов и дочерних организаций (далее – Политика безопасности) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, выработки и совершенствования комплекса согласованных правовых норм, организационно-административных мероприятий и программно-технических средств защиты информационных ресурсов автономной организации образования «Назарбаев Интеллектуальные школы», ее филиалов и дочерних организаций (далее – АОО).

2.Документ разработан в соответствии с требованиями стандарта СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

3.В настоящей Политике безопасности используются следующие основные понятия и определения:

Анализ	Деятельность, предпринимаемая для определения пригодности, адекватности и результативности объекта анализа в достижении заданных целей.
Анализ риска	Процесс понимания характера риска и определения уровня риска. Примечание 1 к определению: анализ рисков включает прогнозную оценку риска. Примечание 2 к определению: анализ риска обеспечивает основу для определения степени риска и принятия решения об обработке риска.

Актив	Связанный со средствами обработки информации, материальный или нематериальный объект, который является информацией или содержит информацию, или служит для обработки, хранения, передачи информации и имеющий ценность для АОО в интересах достижения целей и непрерывности ее деятельности: – информационные активы (базы данных и файлы данных, системная документация и т.д.); – активы программного обеспечения (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты); – физические активы (компьютерное оборудование, оборудование связи, носители информации, другое техническое оборудование, мебель, помещения).
Аудит информационной безопасности	Процесс получения объективных качественных и количественных оценок текущего состояния информационной безопасности АОО в соответствии с определенными критериями и показателями безопасности: -инструментальный анализ защищенности автоматизированной системы. Данный вид аудита направлен на выявление и устранение уязвимостей программного и аппаратного обеспечения системы; – оценка автоматизированных систем на предмет соответствия рекомендациям международных стандартов и требованиям документов СТРК, ГОСТов, отраслевых стандартов; -экспертный аудит защищенности автоматизированной системы. Данный вид аудита направлен на выявление недостатков в системе защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования. Примечание 1 к определению: независимый аудит – внешняя независимая экспертиза, осуществляемая независимыми дипломированными аудиторами, не состоящими в трудовых отношениях с АОО.
Доступность	Свойство информации находиться в состоянии готовности и используемости по требованию авторизованного пользователя.

Идентификация риска	Процесс выявления, определения и описания рисков. Примечание 1 к определению: идентификация риска может включать в себя выявление источников риска, событий, их причин и возможных последствий. Примечание 2 к определению: при идентификации риска могут использоваться данные за прошедший период, аналитические методы, обоснованные мнения и экспертные оценки, а также потребности заинтересованных сторон.
Информационная безопасность (ИБ)	Процесс обеспечения конфиденциальности, целостности и доступности информационного пространства АОО, который определяется отсутствием недопустимых рисков, связанных с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы информационных систем, с поломкой компонентов IT-инфраструктуры АОО, которые могут вызвать перерывы в работе.
Инцидент ИБ	Одно или несколько нежелательных, или неожиданных событий ИБ, которые со значительной степенью вероятности подвергают опасности деловую деятельность и угрожают ИБ.
Конфиденциальность	Свойство, указывающее, что информация остается недоступной или нераскрытой для неавторизованных частных и юридических лиц или процессов.
Мониторинг	Определение состояния системы, процесса или работы. Примечание 1 к определению: для определения состояния может быть необходимым проверять, контролировать или критически изучать.
Надежность	Свойство соответствия предполагаемому поведению и результатам.
Нарушение ИБ	Случайное или преднамеренное неправомерное действие физического лица в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для АОО.
Оценка риска	Единый процесс идентификации риска, анализа риска и определения степени риска.
Политика безопасности	Намерения и направление развития АОО, официально сформулированные высшим руководством.

Риск	Влияние неопределенности на достижение целей. Примечание 1 к определению: влияние – это отклонение от ожидаемого – положительное или отрицательное. Примечание 2 к определению: неопределенность – состояние, даже частичное, нехватки информации, связанной с пониманием события или знанием о нем, его последствий или вероятности. Примечание 3 к определению: риск часто характеризуется указанием возможных событий и последствий, или их комбинации. Примечание 4 к определению: риск часто выражается в форме комбинации последствий события (включая изменения в обстоятельствах) и связанной с ним вероятности возникновения. Примечание 5 к определению: в контексте систем менеджмента ИБ, риски ИБ могут быть выражены как влияние неопределенности на достижение целей ИБ. Примечание 6 к определению: риск ИБ связан с вероятностью того, что угрозы будут реализовываться использованием уязвимости) информационных активов или групп информационных активов и, тем самым, наносить ущерб АОО.
Система менеджмента информационной безопасности (СМИБ)	СМИБ включает в себя политики ИБ, процедуры, руководства и соответствующие ресурсы и задачи, коллегиально управляемых АОО в целях защиты ее информационных активов.
Событие ИБ	Установленное возникновение состояния системы, службы или сети, указывающее на возможное нарушение политик ИБ или недостаточность средств управления, или на ранее неизвестную ситуацию, которая может быть существенной с точки зрения безопасности.
Стандарт обеспечения безопасности	Документ, устанавливающий разрешенные методы обеспечения безопасности.
Требование	Потребность или ожидание, которое сформулировано, обычно подразумеваемое или обязательное. Примечание 1 к определению: “Обычно подразумеваемая” означает, что это специфическая или общепринятая практика для АОО и заинтересованных сторон, когда рассматриваемые потребности или ожидания предполагаются. Примечание 2 к определению: Установленным требованием является такое требование, которое определено, например, в документированной информации.

Угроза ИБ	Потенциальная причина нежелательных или непредвиденных событий, совершенных случайно или преднамеренно, которые могут нанести ущерб информационной безопасности АОО.
Управление ИБ	Система, посредством которой направляются и контролируются действия АОО в сфере ИБ.
Управление доступом	Механизмы, призванные гарантировать, что доступ к активам разрешен и ограничен в соответствии с требованиями бизнеса и безопасности.
Устройства обработки информации	Любая система обработки информации, служба или инфраструктура, или физическое место их размещения.
Уязвимость	Слабое место актива или средства управления, которое может быть использовано одной или более угрозой.
Целостность	Свойство сохранения полноты и точности.

2.Цели ИБ

4. Политика безопасности направлена на достижение следующих целей:

обеспечение доступности информации;
обеспечение целостности информации;
обеспечение конфиденциальности информации;
обеспечение отказоустойчивости и безопасного восстановления данных (резервирование, дублирование, зеркалирование оборудования и данных, резервное копирование и электронное архивирование информации);
обеспечение непрерывности основных бизнес-процессов АОО;
обеспечение защиты авторских прав с использованием возможности существующих технических и программных методов и средств;
определение ответственности пользователей информационного пространства АОО;
выявление уязвимостей объектов защиты и потенциальных угроз ИБ и их исключение либо минимизация потерь и ущерба от нарушений в области ИБ.

3.**Управление ИБ**

5. Для эффективного выполнения указанных целей в АОО действует система менеджмента информационной безопасности (далее – СМИБ) соответствующая рекомендациям международных стандартов линейки ISO/IEC 27000 «Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности».

6. СМИБ документирована в настоящей Политике безопасности, в правилах, процедурах, рабочих инструкциях, которые являются обязательными к исполнению для всех работников АОО в области действия системы. Документированные требования СМИБ доводятся до сведения всех работников АОО.

7. Все объекты защиты ИБ (информационные активы, кадровые активы, материальные активы, сервисные активы и т.д. (далее – Активы) подлежат учету.

8. Для обеспечения ИБ активов применяется риск-ориентированный подход, позволяющий определить и классифицировать риски нарушения ИБ с учетом действующих мер и средств защиты, включая правовые (законодательные), морально-этические, организационные (административные), физические, технические

(программные и программно-аппаратные средства обеспечения СМИБ), а также выявлять, учитывать и реагировать на инциденты в сфере ИБ в соответствии с установленными процедурами.

9. Средства вычислительной техники, корпоративная электронная почта, информационные системы и другие информационные ресурсы, а также вся информация, создаваемая, обрабатываемая и хранящаяся в указанных средствах, являются собственностью АОО.

10. Любая информация, предоставленная источником вне АОО, считается данными от внешних источников. При поступлении таких данных они сопровождаются соглашениями об авторских правах и конфиденциальности, в которых указывается, как использовать эту информацию.

11. Работники АОО получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей.

12.Работники АОО и третьи лица, имеющие доступ к данным в силу выполнения своих служебных обязанностей, подписывают обязательство о неразглашении и сохранности информации.

4.Зоны ответственности участников процесса обеспечения ИБ

13. Подразделение, ответственное за ИБ (далее – Подразделение ИБ), осуществляет:

реализацию мероприятий по оценке рисков нарушения ИБ и защиты информации;
поддержку, мониторинг, анализ и непрерывность улучшения СМИБ;
ознакомление работников АОО в сфере ИБ;
решение вопросов стратегического планирования по ИБ, а также контроль и расследование внештатных ситуаций и инцидентов в области защиты информации.

14. В рамках исполнения настоящей Политики безопасности Подразделение ИБ проводит мониторинг и плановый аудит программно-аппаратного комплекса, обеспечивающего функционирование норм и правил текущего документа и других внутренних регламентирующих документов по ИБ. Мониторинг проводится силами и средствами самого Подразделения ИБ. Независимый аудит ИБ может быть проведен с привлечением независимой аудиторской компании.

15. Сотрудник, ответственный за кадровое делопроизводство АОО несет ответственность за ознакомление работников, использующих ПО, ИС, средства вычислительной техники, с требованиями Политики безопасности под роспись.

16. Администраторы информационных ресурсов АОО обеспечивают непрерывное функционирование информационных ресурсов и корпоративной сети и отвечают за реализацию технических мер, необходимых для приведения в жизнь политик ИБ.

17. Работники АОО несут персональную ответственность за соблюдение требований документов СМИБ, сохранность документации и конфиденциальность информации, ставшей известной третьим лицам в силу выполнения своих служебных обязанностей. Работники обязаны сообщать обо всех выявленных нарушениях в области ИБ Подразделению ИБ.

18. За несоблюдение порядка и правил использования информационных ресурсов к виновным могут быть применены меры, предусмотренные трудовыми договорами, заключенными между АОО, и работником, а также действующим законодательством Республики Казахстан и другими внутренними правовыми и регламентирующими документами АОО.

5. Порядок утверждения и внесения изменений и дополнений в настоящую Политику безопасности

19. Внесение изменений в настоящую Политику безопасности может производится по

результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий

6.Заключительные положения

20. Требования настоящей Политики безопасности дополняются и уточняются другими внутренними правовыми и регламентирующими документами ИБ АОО.

21. Настоящая политика безопасности является общедоступной и предоставляется любому пользователю информационных ресурсов АОО.