«АЛМАТЫ СӘУЛЕТ ЖӘНЕ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР КОЛЛЕДЖІ» ЖШС

ТОО «АЛМАТИНСКИЙ КОЛЛЕДЖ АРХИТЕКТУРЫ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

«УТВЕРЖДАЮ»
Директор колледжа
_____Султанов Н.М.
«___»_____ 2026 г.

ПОЛОЖЕНИЕ
О КИБЕРБЕЗОПАСНОСТИ

Алматы 2026 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Кибербезопасность — это комплекс мер по защите информационных систем, компьютеров, сетей, программ, данных и цифровых сервисов от несанкционированного доступа, кражи или утечки информации, вредоносных программ и вирусов, взлома учетных записей, уничтожения или изменения данных.

1.2. Кибербезопасность в организации включает надежные пароли и двухфакторную аутентификацию, ограничение доступа работников к информации, защиту персональных данных, антивирусную защиту, резервное копирование, правила использования электронной почты и мессенджеров, порядок действий при взломе или утечке данных.

1.3. Кибербезопасность — неотъемлемая часть операционной деятельности Работодателя. Настоящее Положение регулирует порядок использования работниками информационных систем, вычислительной техники, программного обеспечения, корпоративной электронной почты и иных цифровых ресурсов ТОО «АВС» (далее — Компания) и устанавливает требования, направленные на защиту этих ресурсов от киберугроз.

1.4. Требования Положения распространяются на всех работников Работодателя без исключения, независимо от должности, подразделения и формы занятости, в части, касающейся использования информационных ресурсов при исполнении трудовых обязанностей.

1.5. Положение преследует три взаимосвязанные цели: предотвращение киберинцидентов, минимизацию риска несанкционированного доступа к информации и поддержание непрерывной и безопасной работы информационных систем Работодателя.

1.6. Обязанности Работодателя. Работодатель обязан:

1.6.1. обеспечивает введение Положения в действие и знакомит с ним каждого работника под подпись до момента фактического допуска к информационным ресурсам.

1.6.2. назначает ответственное лицо (или несколько лиц), на

1.6.3. внедряет и поддерживает организационные и технические меры защиты информационных систем, от разграничения доступа до контроля используемого программного обеспечения.

1.6.4. обеспечивает регулярное информирование работников о правилах кибергигиены, в том числе при приеме на работу и при существенном изменении угроз.

1.6.5. рассматривает поступающие от работников сообщения об угрозах информационной безопасности и принимает меры по их устранению в разумный срок.

1.6.6. осуществляет внутренний контроль за соблюдением работниками требований настоящего Положения и правил кибергигиены в соответствии с пп. 25-1 п. 2 ст. 23 Трудового кодекса РК.

1.7. Обязанности работников. Работник обязан:

1.7.1. Работник соблюдает требования Положения в полном объеме на протяжении всего периода использования информационных ресурсов Работодателя.

1.7.2. Использование компьютерной техники, корпоративной электронной почты, программного обеспечения и иных информационных ресурсов допускается исключительно в служебных целях, для исполнения трудовых обязанностей.

1.7.3. Логины, пароли и иные средства доступа к информационным системам являются персональными и не подлежат передаче третьим лицам ни при каких обстоятельствах.

1.7.4. Установка любого программного обеспечения на технику Работодателя без предварительного согласования не допускается.

1.7.5. Копирование, передача и распространение служебной информации допускаются только при наличии производственной необходимости. ,

1.7.6. Работник не открывает электронные письма, ссылки и вложения, если их источник

неизвестен или вызывает обоснованные сомнения, независимо от того, насколько убедительно оформлено сообщение.

1.7.7. При обнаружении признаков вредоносного программного обеспечения, попыток несанкционированного доступа, утраты носителей информации либо иных инцидентов информационной безопасности работник незамедлительно информирует ответственное лицо или непосредственного руководителя, до самостоятельного устранения проблемы.

1.7.8. При прекращении трудовых отношений работник возвращает Работодателю все ранее выданные устройства, носители информации, средства доступа и иное имущество, использовавш

1.7.9. Работнику категорически запрещается передавать списки учащихся (студентов), их ИИН, медицинские данные и контакты родителей через незащищенные каналы связи (личные мессенджеры WhatsApp/Telegram, личную почту) третьим лицам.

1.7.10. Работнику запрещается передавать логины и пароли от электронных журналов и образовательных платформ (College SmartNation и др.) коллегам, учащимся или их родителям для совершения действий в системе от своего имени.

1.8. Правила кибергигиены:

1.8.1. Пароли должны быть надежными (состоять не менее чем из 8 символов, включать заглавные и строчные буквы, цифры и спецсимволы) и известны только самому работнику. Фиксация паролей на бумажных или электронных носителях, доступных третьим лицам, не допускается. Смена паролей от учетных записей рабочих компьютеров и образовательных платформ производится не реже 1 раза в 90 дней.

1.8.2. Подключение неизвестных съемных носителей информации к технике Работодателя не допускается.

1.8.3. О неисправностях компьютерной техники и любой подозрительной активности в информационных системах работник сообщает своевременно, не откладывая на конец рабочего дня

1.8.4. Правила кибергигиены применяются наряду с требованиями Положения и не заменяют их

1.8.5. Работникам запрещается загружать служебные документы, локальные акты, а также любые персональные данные учащихся и работников в системы генеративного искусственного интеллекта (ChatGPT и иные публичные нейросети для перевода и редактирования текстов) во избежание утечки информации.

1.9. Ответственность сторон.

1.9.1. Нарушение требований Положения влечет дисциплинарную ответственность работника в порядке, установленном Трудовым кодексом Республики Казахстан.

1.9.2. Если нарушение образует состав административного, гражданско-правового или уголовного правонарушения, виновное лицо привлекается к соответствующей ответственности на основании законодательства Республики Казахстан, независимо от применения дисциплинарного взыскания.

1.10. Заключительные положения

1.10.11. Положение вводится в действие с даты его утверждения работодателем (если утверждается конкретным должностным лицом) или приказом Работодателя и применяется с даты, указанной в приказе.

1.10.12. Изменения и дополнения в Положение вносятся приказом Работодателя и доводятся до работников в том же порядке, что и само Положение.

1.10.13. Положение действует бессрочно, до его отмены либо утверждения в новой редакции.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. При разработке настоящего Положения использованы следующие нормативные документы:

- Закон Республики Казахстан «О персональных данных и их защите».
- Цифровой кодекс Республики Казахстан от 09 января 2026 года № 255-VIII.
- Закон Республики Казахстан «О кибербезопасности» от 24 ноября 2015 года № 418-V ЗРК (в действующей редакции); Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (в редакции от 25.02.2026).
- Закон Республики Казахстан от 24 июня 2026 года № 326-VIII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, защиты персональных данных...».
- Трудовой кодекс Республики Казахстан (с учетом изменений и дополнений, вступивших в силу с 25 августа 2026 года).

3. ЦЕЛИ И ЗАДАЧИ

3.1 Целями обеспечения кибербезопасности в Организации образования являются защита персональных данных учащихся (студентов), их родителей и педагогов, а также обеспечение безопасной работы с государственными и образовательными информационными системами (НОБД, College SmartNation и др.).

3.2 Основными задачами являются обеспечение непрерывности образовательного процесса, предотвращение утечек чувствительных данных и неукоснительное соблюдение законодательства РК в сфере защиты персональных данных и кибербезопасности.