Кабардино-Балкарская Республика
Государственное бюджетное профессиональное образовательное учреждение
«Кабардино-Балкарский колледж «Строитель»

Принято Педагогическим советом
Протокол № 4 от «08» 03 2024г.

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "КАБАРДИНО-БАЛКАРСКИЙ КОЛЛЕДЖ "СТРОИТЕЛЬ"

Подписан: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "КАБАРДИНО-БАЛКАРСКИЙ КОЛЛЕДЖ "СТРОИТЕЛЬ"
DN: C=RU, S=Кабардино-Балкарская Республика, STREET="Промышленный проезд 1-й уд., д.1", L=г.Нальчик, T=ИСПОЛНЯЮЩИЙ ОБЯЗАННОСТИ ДИРЕКТОРА, O="ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ""КАБАРДИНО-БАЛКАРСКИЙ КОЛЛЕДЖ ""СТРОИТЕЛЬ""", ОГРН=1030700203951, СНИЛС=13424275940, OID.1.2.643.100.4=0711030683, ИНН=070703062502, E=stroitei@mail.ru, G=Мурат Русланович, SN=Курманов, CN="ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ""КАБАРДИНО-БАЛКАРСКИЙ КОЛЛЕДЖ ""СТРОИТЕЛЬ"""
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2024-03-01 13:26:33
Foxit Reader Версия: 9.7.1

Утверждено
Приказом ГБПОУ «КБКС»
№ 30 от «01» 03 2024г.
И.о.директора _____ М.Р.Курманов

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах ГБПОУ «Кабардино-Балкарский колледж «Строитель»

г.Нальчик 2024г.

1. Общие положения

1.1 Назначение документа

1.1.1 Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных в ГБПОУ «Кабардино-Балкарский колледж «Строитель»» (далее – Организация).

1.1.2 Положение разработано в соответствии с: Конституцией Российской Федерации; Гражданским кодексом Российской Федерации; Трудовым кодексом Российской Федерации; Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных"; Федеральным законом "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"; Федеральным законом от 22 февраля 2017 г. N 16-ФЗ "О внесении изменений в главу 5 Федерального закона "О персональных данных" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"; Указом Президента РФ № 188 от 06.03.1997 «Об утверждении перечня сведений конфиденциального характера»; иными нормативными актами, действующими на территории Российской Федерации; Указа Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

1.1.3 Цель Положения – регулирование работ по защите персональных данных и обеспечение функционирования информационных систем персональных данных. Организации в соответствии с требованиями действующего федерального законодательства в области информационной безопасности.

2. Понятие и состав персональных данных.

2.1.Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2 Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.3.Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.4.Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5.Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.6.Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.7.Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.8.Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.9.Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.10.Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Цели обработки персональных данных.

3.1. Цель Положения – регулирование работ по защите персональных данных и обеспечение функционирования информационных систем персональных данных. Организации в соответствии с требованиями действующего федерального законодательства в области информационной безопасности. Обеспечение соблюдения законодательства РФ в сфере образования.

3.1.1. Персональные данные работника - информация, касающаяся конкретного работника, которая необходима колледжу в связи с отношениями, возникающими между работником и колледжем.

3.1.2. К персональным данным работника относятся: сведения, содержащиеся в документах, удостоверяющих личность; информация, содержащаяся в трудовой книжке; документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС); сведения, содержащиеся в документах воинского учета; сведения о наличии/отсутствии судимости; сведения об образовании, квалификации или наличии специальных знаний или подготовки; информация о состоянии здоровья в случаях, предусмотренных законодательством; сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе

на территории Российской Федерации; сведения о семейном положении; адрес электронной почты; адрес регистрации; номер телефона; гражданство; данные документа, содержащиеся в свидетельстве о рождении; справки с места учебы детей; справки о составе семьи; . Информация о заработной плате; информация, необходимая для предоставления гарантий и компенсаций, установленных действующим законодательством; документы бухгалтерского учета, реквизиты банковских карт; номер расчетного счета; номер лицевого счета содержащие информацию о расчетах с персоналом; медицинские документы, справки;

3.1.3. Персональные данные обучающихся – информация, касающаяся конкретного обучающегося, которая необходима колледжу в связи с отношениями, возникающими между обучающимся и/или их родителями (законными представителями) и колледжем.

3.1.4. К персональным данным обучающихся относяться : сведения, содержащиеся в документах, удостоверяющих личность; документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС); сведения, содержащиеся в документах воинского учета; сведения об образовании, информация о состоянии здоровья в случаях, предусмотренных законодательством; сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации; сведения о семейном положении; адрес электронной почты; адрес регистрации; номер телефона; гражданство; данные документа, содержащиеся в свидетельстве о рождении; справки о составе семьи; реквизиты банковских карт; номер расчетного счета; медицинские документы, справки;

4. Область действия документа

4.1. Действие Положения распространяется на информационные системы персональных данных Организации, в которых осуществляется обработка персональных данных.

4.2. Все работники Организации, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись.

5.Вступление в силу документа

5.1. Настоящее Положение вступает в силу с момента его утверждения руководителем и действует бессрочно до замены его новым Положением.

5.2. Все изменения в Положение вносятся приказом руководителя.

6. Организация и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

6.1. Планирование работ по обеспечению безопасности персональных данных .

6.1.1. В целях исполнения настоящего Положения ответственный за защиту ПДн и администратор безопасности составляет и утверждает у руководителя план работ по обеспечению безопасности персональных данных, обрабатываемых в Организации.

Проводимые в Организации мероприятия по обеспечению безопасности персональных данных учитываются в плане мероприятий по защите персональных данных в Организации.

6.1.2.Выполнение работ по обеспечению безопасности персональных данных

6.1.3. В целях организации и проведения работ по обеспечению безопасности персональных данных в Организации приказом руководителя назначаются:

- лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности;
- администратор информационной безопасности, ответственный за установку, настройку и обслуживание средств защиты информации, применяемых в Организации для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными;
- комиссия по проведению классификации информационных систем.

6.1.4. Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности персональных данных:

- определение и описание информационных систем персональных данных;
- классификацию информационных систем персональных данных;
- определение актуальных угроз безопасности персональных данных;
- проектирование системы защиты персональных данных, включающей организационные, физические и технические меры и средства защиты;
- закупку, установку и настройку технических средств защиты информации;
- внедрение организационных мер и разработку соответствующих регламентов и положений;
- инструктаж и обучение лиц, которые будут использовать средства защиты информации.

6.1.5. Начальники отделов, в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований Положения об обработке персональных данных и других установленных в Организации требований.

6.1.6. Для обеспечения безопасности персональных данных в Организации применяются следующие меры безопасности:

- организационные меры безопасности:
    - инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;
    - учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;
    - мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;
    - постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);
- меры физической безопасности:
    - ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом руководителя устанавливается контролируемая зона, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения Организации с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;
    - размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
    - организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
- технические меры безопасности:
    - разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
    - регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
    - резервирование технических средств, дублирование массивов и носителей информации;
    - использование защищенных каналов связи;
    - предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

6.1.7. Ремонтно-восстановительные работы технических средств обработки информации

проводятся администратором безопасности. В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

6.2. Контроль выполнения работ по обеспечению безопасности персональных данных

6.2.1.Контроль выполнения работ по обеспечению безопасности персональных данных в Организации (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

6.2.2. В рамках проведения контрольных мероприятий выполняются:

проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;

проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;

проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;

проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

6.2.3. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

6.2.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению руководителя и в случае возникновения инцидентов информационной безопасности.

6.2.5. Внутренние проверки в Организации в обязательном порядке проводятся в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;
- халатность и несоблюдение требований к обеспечению безопасности персональных данных;
- несоблюдение условий хранения носителей персональных данных;
- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

6.2.6. Задачами внутренней проверки являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

6.3. Совершенствование системы защиты персональных данных

6.3.3. Ежегодно ответственный за защиту персональных данных предоставляет руководителю отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

6.3.4. Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

- результатами проведенных аудитов и контрольных мероприятий;
- изменениями федерального законодательства в области персональных данных;
- изменениями структуры процессов обработки персональных данных в пенсионном фонде;
- результатами анализа инцидентов информационной безопасности;
- результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;
- жалоб и запросов субъектов персональных данных.

6.3.5. На основании решения, принятого руководителем по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ответственный за защиту персональных данных составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Организации, на следующий год.